DISCUSSION DRAFT
7-16-02

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT

Model County Technology Architecture

July 16, 2002

MTG Management Consultants, L.L.C.
1111 Third Avenue, Suite 2700
Seattle, Washington 98101-3201
206.442.5010 206.442.5011 *fax*
www.mtgmc.com

TABLE OF CONTENTS

TABLE OF CONTENTS

(continued)

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

The Wisconsin Justice Information Sharing (WIJIS) effort has defined business and technology requirements necessary to improve the sharing of information between existing and future criminal justice information systems (CJISs). The pilot implementation project for this effort is referred to as the Model County project. The Model County team is working on the technology architecture to satisfy these requirements. The Model County architecture, once validated and funded, would subsequently be propagated to the other counties in Wisconsin. In support of this project, several design documents, including this Technology Architecture report, are being created. The focus of the Technology Architecture is solely on the Model County project. In short, this document specifies technology that will satisfy the project vision, goals, and previously specified requirements. This report will also lead to the Implementation Road Map deliverable that provides the outline for implementing the technology and achieving the desired results.

The scope of this project is defined by three key components: linking PROTECT to the Circuit Court Automation Program (CCAP), linking law enforcement agencies to PROTECT, and providing a Web-based lookup of PROTECT data for participating law enforcement agencies. The vision, goals, scope, and principles of this project are defined in the Business Requirements document and summarized in Section II herein.

The strategic decisions outlined in Section III of this report provide guidance for the technology architecture and implementation strategy. These decisions resolve most of the key issues identified in the Business Requirements document. They have been categorized as relating to business, management and governance, and technology decisions and are the framework for the technology architecture.

Section IV of the document provides a high-level overview of the technology principles and resulting architecture. This section presents the conceptual framework that is used to detail the technology architecture. The models presented in Section IV provide the perspective necessary to understand the organization of the architecture and the supporting architecture and design packets that provide the architecture's design details.

The remainder of the document discusses three increasingly detailed layers of the architecture. Sections V through VII provide the architecture layers and APPENDICES C through H provide architecture packets and supporting design packets, where appropriate, that add detail to specific architectures.

The Technology Architecture document is intended to provide the baseline design that will become the Model County project's implemented technology architecture. It is organized in updateable sections that can be revised as each portion of the architecture is built and implemented to provide a useable, long-term design document that is used in support of maintenance and enhancements to the environment.

I. INTRODUCTION

I. INTRODUCTION

This document presents the technology architecture for the Wisconsin Justice Information Sharing (WIJIS) Model County project. This is a narrowly defined effort to test Web-based technologies and the state's ability to implement them in support of real-world need, moving information to and from local law enforcement. It is important to understand that the project follows this narrow path without intending to imply larger, more global WIJIS direction. However, there are larger, longer-term WIJIS issues that the Model County project addresses in the effort to provide a consistent design and implementation that can be replicated in other Wisconsin counties. The Model County project architecture establishes a number of choices because of the restricted grant time frame that may later be adopted or modified when WIJIS reaches those decision points. The Model County architecture does provide a flexible, capable design to implement the Model County and grow with WIJIS in the future.

A. BACKGROUND

Last year, Wisconsin was awarded a grant from the National Governors' Association (NGA) to complete this project. A project team was formed, and initial design decisions were made related to the use of both eXtensible Markup Language (XML) for data transport definition and Simple Object Access Protocol (SOAP) for system communications and interoperability. The project team requested assistance with the overall design of the infrastructure within the initial Model County and with the planning for continued implementation in other counties. MTG Management Consultants, L.L.C., was selected to provide the assistance desired by WIJIS.

Over the last 3 months, MTG, WIJIS personnel, and other state staff have reviewed the technical and application infrastructure available for the Model County project. Several components of the infrastructure have been discussed, including BadgerNet, overall network connectivity, security, specific pilot county organization and systems, Circuit Court Automation Program (CCAP), District Attorney (DA) PROTECT, and CCAP's Simple Transaction Exchange Protocol (STEP) Message Oriented Middleware (MOM) technology. Green Lake and Jefferson counties have been selected as the Model County pilot sites.[1] These two counties provide the best mixture of environments for the test. In addition, alternative products and approaches have been reviewed for their applicability to the Model County project.

[1] The selection of a second county is still under review, but it is currently expected that Jefferson County will be chosen.

B. APPROACH

The Model County architecture is based on the two recent draft documents that have been circulated to WIJIS. The WIJIS Concept Paper and the Model County Business Requirements documents created several weeks of discussion and were used to frame the information presented in this document. In addition, MTG has developed the architecture using our method of presenting the information and the best practices that we have observed around the country. EXHIBIT I-1, which follows this page, depicts the project planning approach and various project deliverables. The resulting analysis and decisions are detailed in this architecture along with the technologies that will support the Model County project.

The Technology Architecture document is designed to provide the framework for a complete architectural design that contains all of the architectural structure for the Model County and later WIJIS. The framework provides the conceptual information in this release that can be replaced with an implemented design document once the project is completed. The key to maintaining the environment is adding each interface or major component project that is implemented. The structure of the document is outlined in the next subsection.

C. REPORT ORGANIZATION

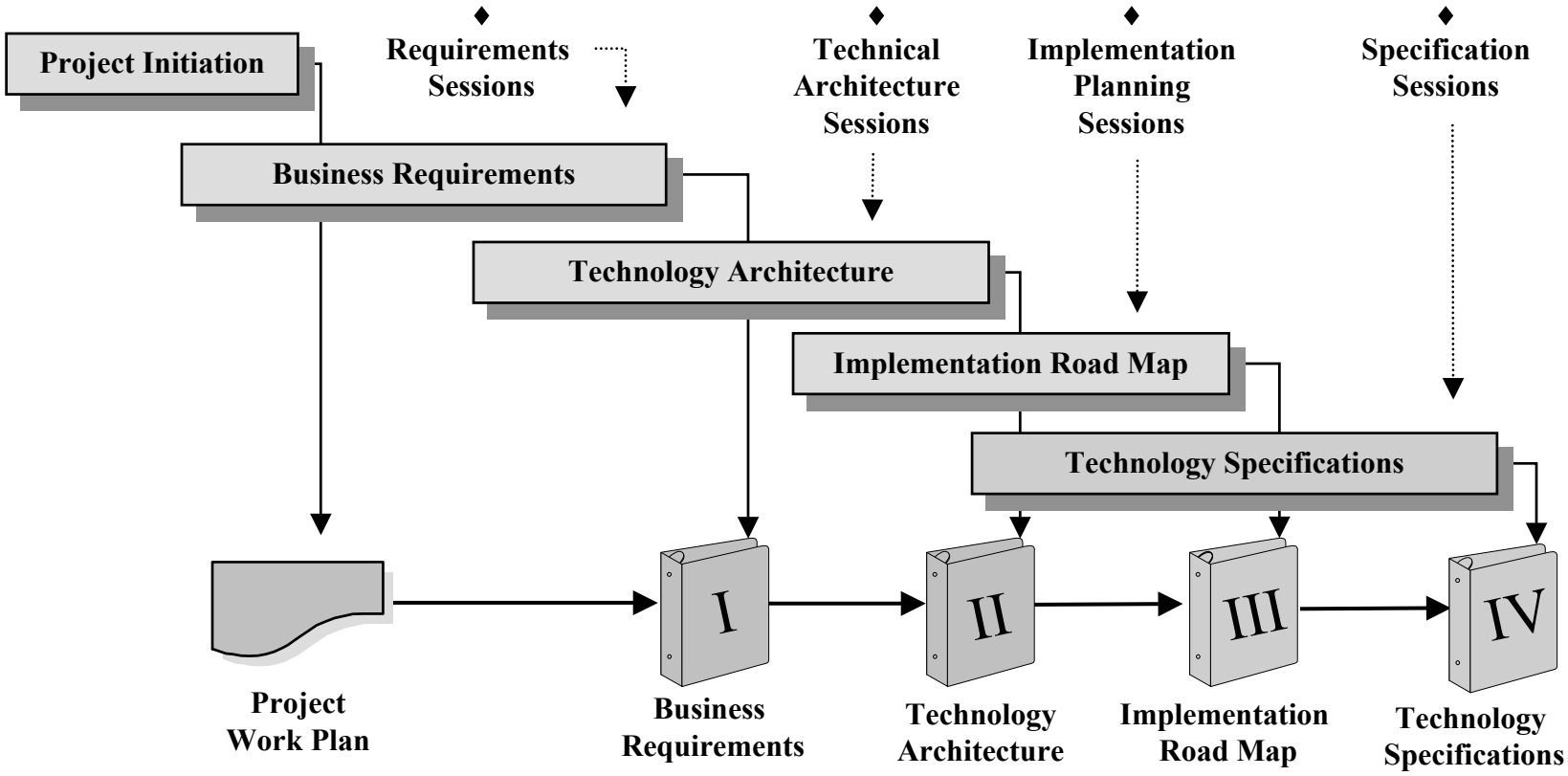
The sections and appendices in this report combine to present the technology architecture for the Model County environment. The report is the second of four deliverables that will define a technology for the Model County project.

The remainder of this document is organized as follows:

- Section II describes the vision and goals for the Model County project.
- Section III discusses the business and technology decisions that have been made in support of the Model County project.
- Section IV provides a set of fundamental technology principles that will guide the development of the Model County and presents the context within which the technology architecture will be described.
- Section V outlines the infrastructure architecture.
- Section VI describes the Model County application, publication, integration, and analysis architectures.
- Section VII discusses the technology management and support standards, systems, and organization required to sustain and enhance the future information-sharing systems.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

PLANNING APPROACH



This document also contains these appendices:

- APPENDIX A – A glossary of acronyms used in the document.
- APPENDIX B – A bibliography of source materials.

In addition, several architecture and design packets are included as part of this Technology Architecture. These packets are intended to provide specific parameters for each component of the architecture. The utility of the packets is intended to extend beyond this document into an actual design portfolio consisting of these packets and future packets created in support of specific Model County or even WIJIS components. The following packets have been provided with this deliverable:

- Infrastructure Architecture Packet (*APPENDIX C*).
  - » Information-Sharing Topology Design Packet (*APPENDIX C-1*).
  - » Equipment Area Design Packet (*APPENDIX C-2*).
  - » Security Architecture Design Packet (*APPENDIX C-3*).
- Application Architecture Packet (*APPENDIX D.*)
  - » Web Site Design Packet (*APPENDIX D-1*).
- Publication Architecture Packet (*APPENDIX E*).
  - » Data Access Design Packet (*APPENDIX E-1*).
- Integration Architecture Packet (*APPENDIX F*).
  - » Message Exchange Design Packet (*APPENDIX F-1*).
- Analysis Architecture Packet (*APPENDIX G*).
- Management Architecture Packet (*APPENDIX H*).
  - » Security and User Database Design Packet (*APPENDIX H-1*).
  - » Auditing and Logging System Design Packet (*APPENDIX H-2*).

This structure provides the framework for a complete architectural design document, provided that information is documented and added with each Model County component.

II. VISION AND GOALS

II. VISION AND GOALS

The initial step in developing the Model County project was to identify the business goals and supporting technology goals upon which the project vision was defined. Specific technology-related initiatives and tactical projects will be based upon implementation of the project vision. This section discusses the justice stakeholders that will be served, the vision for the Model County effort, and the business and enabling technology goals that can be used to guide and measure progress in implementing the technology architecture. It is organized under the following headings:

- *Customers* – Customers are the recipients and beneficiaries of the results of any new technology acquired through implementation of this plan.
- *Vision* – The vision statement expresses the desired future state of justice community operations and systems when the Model County effort is implemented.
- *Financial Principles* – These principles briefly state the financial goals of the justice community's Model County project.
- *Business Principles* – These principles briefly state the business objectives of the Model County project.

These statements about the future provide a strategic business technology framework within which specific technology change initiatives and plans of action will be developed.

A. CUSTOMERS

The organizations involved in the Model County effort include:

- Department of Electronic Government (DEG), WIJIS, DA Information Technology (IT).
- CCAP, Director of State Courts Office.
- Crime Information Bureau (CIB), Department of Justice.
- Wisconsin District Attorney Association (WDAA).
- Green Lake County.
- Jefferson County.
- Local law enforcement agencies.

Other user groups may benefit from the Model County effort; however, they are not considered within the scope of this document.

B. VISION

The vision for the WIJIS project is to "enhance the operating efficiencies of each of the individual justice partner organizations for the improvement of justice administration through electronic sharing of information." The goals listed below ensure that the Model County project is in line with the overall WIJIS vision.

- Identify opportunities to electronically share information between WIJIS partners, along with the data elements to be accessed and exchanged.
- Identify and recommend ways to eliminate barriers to electronic sharing and accessing of information.
- Develop, recommend, and promote standards that will facilitate the electronic sharing of information between WIJIS partners.

These goals focus on information sharing within the justice environment and the technology necessary to support that sharing. In support of the above goals, the Model County has been limited to implementing three key components:

- Linking PROTECT to CCAP.
- Linking law enforcement agencies to PROTECT by creating a prototype data transport tool (SOAP/XML) to share data.
- Providing a Web-based lookup of PROTECT data for participating law enforcement agencies.

These components define the scope of the Model County project. The scope restrictions are intended to keep the Model County effort defined and measurable so that the ability to replicate the Model County topology can be evaluated and forecasted for future efforts.

C. FINANCIAL PRINCIPLES

The financial principles represent the desired financial attributes of Model County project. The principles identified below complement the existing mission, priority, and goal statements

established for WIJIS and, more specifically, the Model County project. The Model County financial principles provide direction to the implementation teams and are an important tool for decision makers as issues surface about options, direction, and priorities. The financial principles are:

- Constrain the WIJIS effort with the NGA grant funds.
- Limit the financial impact to local WIJIS partners.

Given these two principles, the technology architecture must constrain both the cost and the necessity to manage and support a large, complex technology infrastructure.

D. BUSINESS PRINCIPLES

The business principles represent the business justification and purpose of Model County project. The principles provide business direction and guidance to the implementation teams and are an important tool for decision makers as issues surface about options, direction, and priorities. The business principles are described below.

- Ensure that there are no requirements on the part of Model County justice partners to change the way they are currently doing business or their technologies.
- Focus on the operational business needs as the primary reason for implementing the WIJIS solution.
- Minimize the business and resource impact on all WIJIS partners.
- Implement a solution that is:
  - » Easy to support.
  - » Able to use open standards.
  - » Replicable.
  - » Scalable.
- Maximize the use of available staff skills.
- Employ a long-term implementation strategy.
- Successfully complete the project before the end of the grant period, October 2003.

Given these seven principles, the technology architecture should focus on the operational goal of effectively sharing information between local justice partners. The effort should be constrained by

both the work necessary at the local level to implement the interfaces and the necessity to change or modify existing partner systems. In addition, the effort should employ a long-term strategy that maximizes the results of the Model County project.

* * * * * *

Accomplishing the Model County project within these guiding principles will provide Wisconsin with a solution for local information sharing that all state and local WIJIS partners can utilize and enhance.

III. STRATEGIC DECISIONS

III. STRATEGIC DECISIONS

The vision, goals, and financial and business principles described in the preceding section form the basis from which the Model County environment is developed to implement the desired information sharing systems. The technology vision and subsequent implementation planning must provide a reasonable approach to moving forward and will be driven by a set of strategic decisions. The decisions documented in this section provide guidance for the technology architecture and implementation strategy. These decisions resolve most of the key issues identified in the Business Requirements document. These strategic decisions have been categorized as relating to business, management and governance, and technology.

A. BUSINESS DECISIONS

The business decisions focus on the issues that guide the Model County project implementation and pilot effort and provide the critical framework for the information exchanges within the scope of the project. The following decisions have been reviewed with the Model County project team during the technology architecture phase of the project.

- Green Lake County will be the primary Model County site, with participation from the Sheriff's Office and agencies supported by the sheriff and Markesan Police Department.
- The Green Lake connection will be based only on BadgerNet connections to minimize possible complexity.
- A second county will be selected to validate extensibility, and that county will include BadgerNet and Internet connections.
- Law enforcement transfers within the Model County project are limited to arrest, charge, victim, and narrative information, as well as disposition information from PROTECT.
- Information lookup queries within the Model County project are limited to in-county PROTECT information only.
- Close monitoring of the expenditures and project status will occur at the level necessary to meet the federal grant requirements.
- When feasible, the environment will be extended to include "No Prosecute" information exchanges with CIB to provide added benefit to law enforcement.

These decisions were discussed by the WIJIS Model County team on May 30, 2002. The business decisions are facilitated by the management and governance decisions outlined in the next subsection.

B. MANAGEMENT AND GOVERNANCE DECISIONS

Strategic management and governance decisions concern the direction of resources within the state for implementation of the Model County project. Decisions affecting Model County management are discussed below.

- Support of the technology is limited to available staff for the Model County project.
- The information exchange topology for the Model County project will be supported from 8 a.m. to 5 p.m., Monday through Friday.
- Model County project decisions will be made by the WIJIS director.
- The WDAA IT subcommittee will determine the appropriate levels of access for PROTECT information.
- The CCAP steering committee will resolve any access issues for CCAP information.
- The Chief's and Sheriff's Association will resolve any access issues for law enforcement organizations.
- Periodic audits of the security and information transfers will occur, focusing on each aspect individually.

These decisions were also discussed by the WIJIS Model County team on May 30, 2002. The management and governance decisions are facilitated by the technology decisions discussed in the next subsection.

C. TECHNOLOGY DECISIONS

Strategic technology decisions concentrate on setting the technology direction for the Model County project. These decisions affect the infrastructure, applications, and technical support environment that will enable improved information access and sharing within the justice community using the Model County implementation. These technology decisions are discussed below.

- The Model County project will utilize Web services as the primary information exchange technology.

- Technology choices and practices will adhere to existing standards unless specific business needs dictate otherwise.
- The development platform will be Microsoft's .NET framework and BizTalk.
- The methods used with the .NET framework will be:
  - » XML for data transport.
  - » SOAP for transport management and control
  - » Web Service Description Language (WSDL) for service definition and access.
  - » Public Key Infrastructure (PKI) for transport security.
  - » Secured virtual private networks (VPNs) for network privacy.
- A Web-based lookup for PROTECT information will be created within a Web portal that can be accessed by Model County users.
- The existing CCAP and PROTECT interface will be maintained until it is feasible to migrate to the new CCAP SOAP interface, at which time that interface will be implemented.
- Existing BadgerNet and Internet connections will be used to provide physical transport. It is important to note that these connections will be secured by a VPN, as noted above.

The decisions outlined in this section were also discussed by the WIJIS Model County team on May 30, 2002.

* * * * * *

The decisions outlined in this section ultimately frame the strategic technology vision, definition of tactical designs, implementation schedules, and overall cost of the plan. Of course, several tactical decisions will be required as the project is initiated and proceeds toward implementation.

IV. TECHNOLOGY ARCHITECTURE OVERVIEW

IV. TECHNOLOGY ARCHITECTURE OVERVIEW

The Model County architecture consists of logically consistent principles and decisions that guide the engineering of the technology infrastructure. Wisconsin intends to establish a common technology model that will create coordinated and common information-sharing services between law enforcement and PROTECT. This section presents an overview of the role and structure of the architecture, sets forth the principles that direct the technical and management components of the future environment, and outlines the manner in which the technology architecture will be discussed.

A. INTRODUCTION

An architecture is a complex compilation of hardware, software, telecommunications, organizations, policies, and procedures. Many organizations, including DEG and many state organizations, maintain a de facto architecture that evolves as technology decisions and acquisitions are made. Although the size, shape, complexity, and capabilities of the WIJIS architecture are not defined, the Model County project structure is defined. This section focuses on defining the Model County technology environment as a result of a long series of coordinated technology decisions that:

- Define a set of principles for making technology decisions.
- Provide a framework and structure for understanding and communicating the major components of the Model County technology architecture.

This framework is discussed in more detail below, first in terms of the technology principles and then in the context of the specific technology architecture framework.

B. TECHNOLOGY PRINCIPLES

WIJIS has adopted a series of principles to direct its management of technology for the Model County project. These principles are derived from the project's vision, goals, and business principles. They also guide decisions about what information technologies will be used and how they will be employed and serve to shape the technology decisions that are made in realizing the Model County vision. Model County technology principles are explained below.

- Ensure that the Model County project follows state standards whenever possible.

  The standards and technology choices will be based on vendor-neutral standards where available and able to be implemented. Model County infrastructure additions implemented by

partner agencies will be compliant with the architecture even though there may be some additional cost for architectural compliance on initial implementation. Within the scope of the Model County project, these costs have been budgeted. Any technological deviations may create a significant impact on efforts during implementation and should be avoided.

- Utilize existing technologies wherever possible.

  The Model County project will rely on existing BadgerNet and Internet connections, existing technologies such as CCAP's STEP interface, and partner systems. The Model County project is not intended to build new infrastructure where that infrastructure is already in place.

- Build the environment with commercial off-the-shelf (COTS) software and hardware.

  The design will be based upon current and developing industry standards to ensure compatibility with future technology. It is important to note that even though specific vendor products will be employed, the resulting environment will follow open industry standards. This includes the underlying messaging environment, as well as the application software used within the Model County framework.

- Secure the environment in accordance with applicable justice security standards and best business practices for justice security.

  A critical element of the Model County project is the security component of the environment. In order to best secure the environment and meet all applicable security and privacy requirements, the Model County project will follow the security practices of national and state justice agencies.

- Implement the solution in accordance with applicable national justice standards and best justice business practices wherever possible.

  The Model County solution will also utilize the best application practices of the justice community. Although many of the technological areas within the Model County are leading edge, the topology and overall design practices can be compared with other successful efforts. These efforts will be used to guide and implement the Model County solution.

- Create a solution with robust management features.

  Management of the Model County environment will be essential for user acceptance and the ability to replicate the solution. Specific management capabilities should include:

  » Monitor specific information exchange status.

» Audit information exchanges at all points from the receipt of the exchange to confirmation that it was accepted by the receiving system.

» Control timing of specific exchanges so that alerts can be generated when timing requirements are exceeded.

» Build complex exchange conditions that generate flexible management notifications if parameters match, such as timing measurements for benchmarking.

» View information exchanges in a graphical level to allow for easy support and maintenance with key business representatives.

These types of management features will minimize the level of effort required to trouble-shoot, maintain, and enhance the environment.

■ Ensure that the environment is scalable.

The design must be able to migrate or grow over time as new requirements are identified and defined and transaction volumes increase. This includes support of the process of introducing new extensions and software releases into existing operational environments. In addition, the system should be developed in a way that recognizes the need for future changes to functional and technology requirements even if the development cost is increased.

Based upon these principles detailed above and the goals outlined in Section II, the technology architecture described in subsequent sections of this document is intended to provide a blueprint for building the technology infrastructure necessary to complete the Model County project. The development of technical plans and product decisions requires considerations of these principles and of the key qualities and attributes that need to be built into an architecture plan.

C. TECHNOLOGY ARCHITECTURE FRAMEWORK

EXHIBIT IV-1, which follows this page, provides a framework for discussion of the Model County technology architecture presented in subsequent sections and follows the principles previously outlined. The overall framework presented in EXHIBIT IV-1 is divided into three primary layers:

■ Infrastructure

This layer of the schema represents hardware that will be employed to facilitate the overall architecture for the Model County.

» Information-Sharing Topology Design.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

TECHNOLOGY ARCHITECTURE FRAMEWORK

Infrastructure

Application,
Publication, Integration,
and Analysis

Management and Support

Components

- Information-Sharing Topology Architecture
- Equipment Area Architecture
- Security Architecture

- Application Architecture
- Publication Architecture
- Integration Architecture
- Analysis Architecture

- Policy Requirements
- IT Organization
- IT Management Tools

» Equipment Area Design.[2]

» Security Architecture Design.

These layers are important to the overall functions of the environment; however, they are not the focus of operational decision makers.

■ Application, Publication, Integration, and Analysis

This layer of the schema is the most visible to the organization and includes:

» *Application Architecture* – The software that supports Model County business functions and information-sharing activities.

» *Publication Architecture* – The data that is compiled and manipulated in support of business activities within the Model County environment.

» *Integration Architecture* – The technology design that supports the information exchanges and messaging needs of the Model County environment.

» *Analysis Architecture* – The analysis systems design that supports the complex data manipulation needs of the Model County environment. This architecture is outside the scope of the Model County project but is mentioned to maintain consistency between the Model County and possible extensions to this architecture.

These architectures create the rule-based intelligence within the information-sharing topology. The level of integration achieved will largely be based on the integration, publication, and application layers.

■ Management and Support

The management architecture layer of the schema represents the technology business management of the future architecture. The components being examined are:

» Policy Requirements.

» IT Organization.

» IT Management Tools.

The management and support layer includes specific designs to audit and secure the user activity within the information-sharing topology.

---

[2] Within the context of the Model County project, this is a single rack or two of equipment that will be collocated in an existing secured facility.

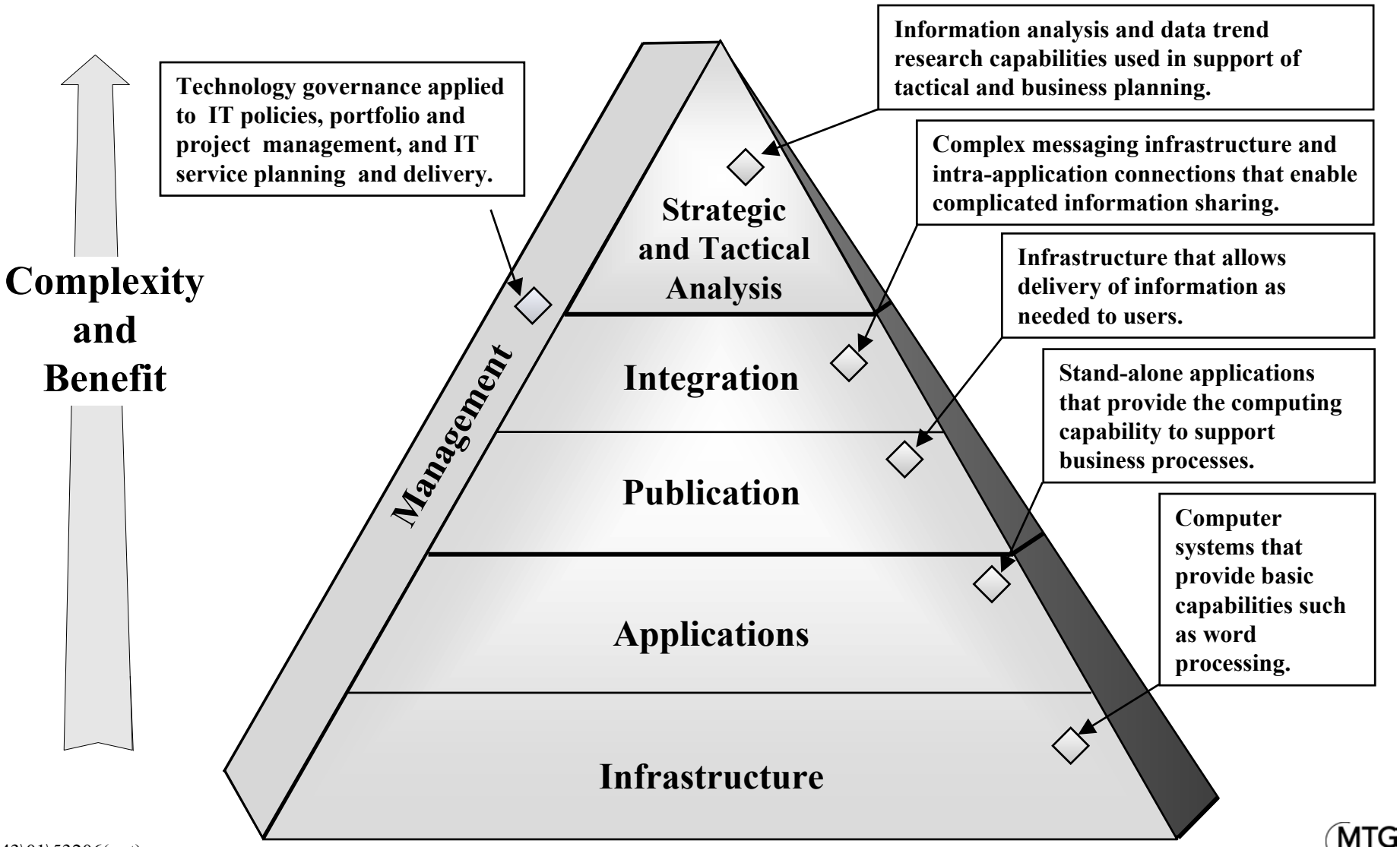
The layers described above parallel MTG's integration model that has been discussed with the Model County project team and is presented in EXHIBIT IV-2, which follows this page. The next three sections discuss the specific architecture layers for the Model County in the context of this framework, beginning with the infrastructure layer and working through the schema to the management and support layer. The discussion is presented in terms of an executive overview of each architectural area or model layer, with references to the detailed architecture and design packet appendix for that layer. Although not all layers have design packets, each supporting architecture appendix is discussed in terms of vision, principles and standards, design decisions, and discussion notes, as described below.

- *Vision* – The purpose of the design packet component is outlined by the vision. In short, the vision provides the guiding rationale for the technology defined in the packet.
- *Principles* – The principles provide the guidelines that frame the design packet component.
- *Design Decisions* – Any design decisions that have been applied to the design will be listed within the design document.
- *Discussion Notes* – These include any issues created by the infrastructure component design or additional tactical decision points that are relevant to complete the understanding of a design packet component.

These discussions are provided in an appendix format, called architecture and design packets, to facilitate the creation of a working technology architecture that is updated and enhanced by revising or adding packets as the components are implemented. EXHIBIT IV-3, which follows EXHIBIT IV-2, depicts the architecture and design packet relationships.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

INTEGRATION MODEL

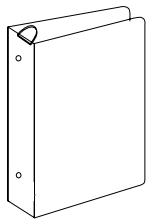


MTG

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

TECHNOLOGY ARCHITECTURE BLUEPRINT

Model County Technology Architecture



Architecture Packets

Architecture Packets

- Infrastructure Architecture
- Application Architecture
- Publication Architecture
- Integration Architecture
- Analysis Architecture
- Management Architecture

Design Packets

- Information-Sharing Topology
- Equipment Area
- Security Architecture
- Web Site
- Data Access
- Message Exchange
- Security and User Database
- Auditing and Logging

V. INFRASTRUCTURE ARCHITECTURE

V. INFRASTRUCTURE ARCHITECTURE

The Model County infrastructure architecture is a blend of the existing technologies and a few critical devices necessary to support the exchanges and secure the environment. The additional infrastructure is part of the overall design explained below. In addition, this section outlines the specific design packets that support the infrastructure model. The infrastructure architecture provides the computing resources for the exchanges within the Model County information-sharing topology.

A. INFRASTRUCTURE MODEL

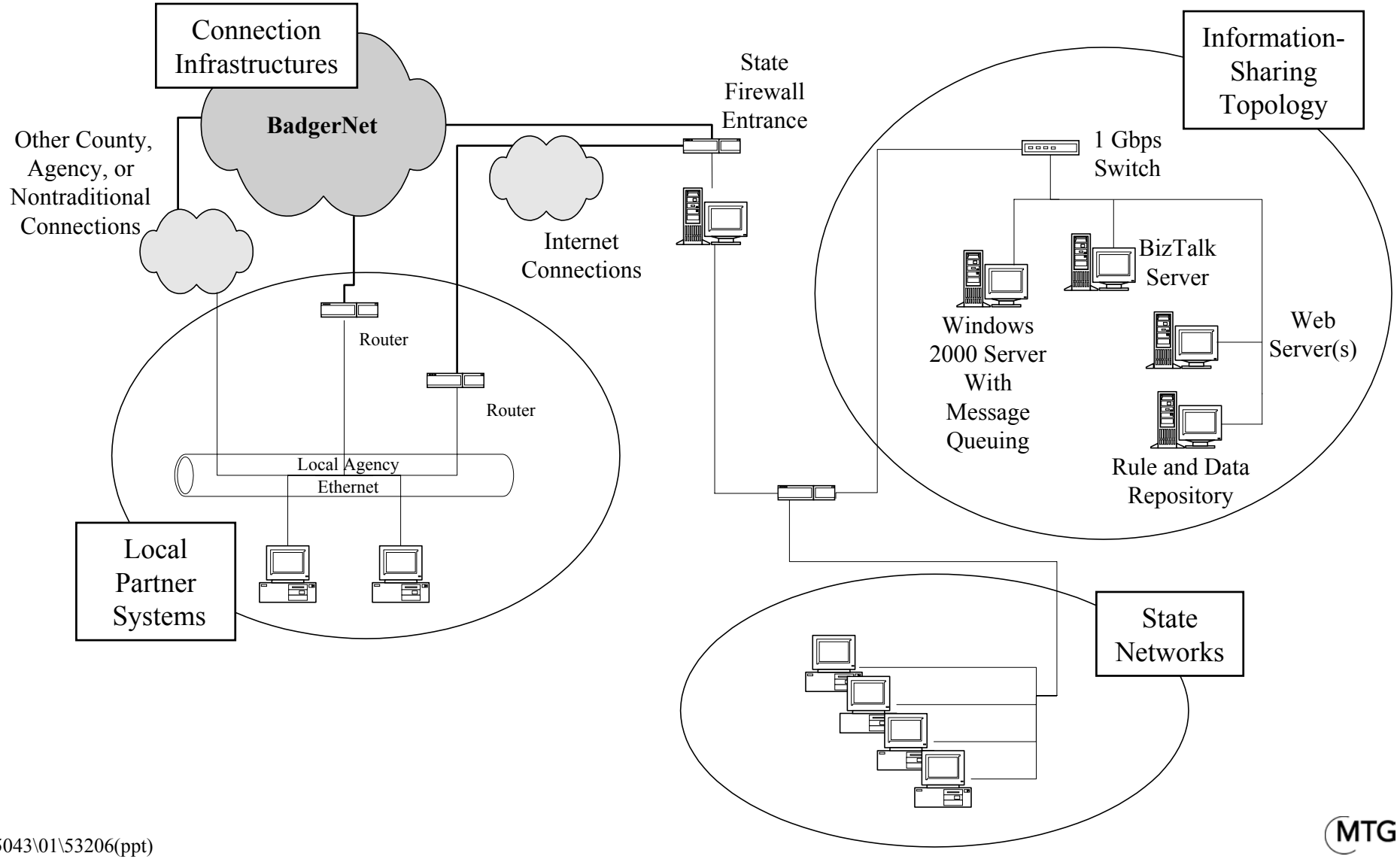
The infrastructure model is largely based on the current infrastructure, but will include additional features needed to support improved security, performance, and availability in the Model County environment. These improvements add Model County information-sharing servers into a WIJIS equipment area and create a secured information-sharing topology. EXHIBIT V-1, which follows this page, is a diagram of the logical infrastructure architecture. Characteristics of the key elements in this future platform model include:

- *Local Partner Systems* – The Model County project focuses on delivering PROTECT information[3] to partners. This component of the model represents the local users and, in cases where local systems exist, those systems as well.
- *Connection Infrastructures* – The connection infrastructures provide the means of accessing the Model County environment and may consist of any secured connection.
- *Information-Sharing Topology* – The information-sharing topology is a logical representation of the WIJIS equipment area, network components, and security mechanisms. Within the context of the infrastructure architecture, this component represents the servers and support systems within the equipment area.
- *State Networks* – This component represents the existing organization infrastructure, including networks, security systems, servers, and client devices. Partner organizations are also represented within this component. For the purposes of the infrastructure architecture discussion, this represents only the server and client systems in this component.

[3] The scope of the Model County project is limited to PROTECT information, but the architecture can be easily extended to offer other information resources should WIJIS be authorized to provide that information.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

LOGICAL INFRASTRUCTURE ARCHITECTURE



These major components are important to the discussion of the infrastructure model. The direct impact of the infrastructure architecture applies to the information-sharing topology; however, the other components of the model are affected by the overall Model County direction. APPENDIX C, the Infrastructure Architecture Packet, provides the architecture and design details for the infrastructure layer.

VI. APPLICATION, PUBLICATION, INTEGRATION, AND ANALYSIS ARCHITECTURES

VI. APPLICATION, PUBLICATION, INTEGRATION, AND ANALYSIS ARCHITECTURES

This section describes the target application, publication, integration, and analysis architectures for the Model County that will support information exchange between and among the justice systems within the scope of the Model County project. The specific architectures are:

- *Application Architecture* – The application architecture is discussed first since the applications provide the inquiry capabilities that support operations and information sharing within the justice community.
- *Publication Architecture* – Next, a logical view of the publication architecture is presented that outlines how the future Model County will support functional operational data needs as well as interfunctional information sharing.
- *Integration Architecture* – The integration architecture is presented third. This architecture describes how key components of the overall Model County technology architecture will support integration and information sharing.
- *Analysis Architecture* – This section concludes with the analysis architecture, which describes how the Model County technology architecture is extensible to support future analysis efforts.

The subsections below support the overall technology principles previously outlined in Section IV and present the high-level explanation of that specific layer of the integration model and Model County technology architecture.

A. APPLICATION ARCHITECTURE

Applications provide the information that is shared within the Model County environment. In addition, the publication layer relies on a specific common design method that is articulated in this architecture. The application architecture presented in APPENDIX D represents the future application design that will support operations for the Model County and most likely within WIJIS. It is important to note that the current vision is not implementing any applications for the Model County project; however, the common design is a necessary component to ensure a common look and feel within the project services that are built.

B. PUBLICATION ARCHITECTURE

A publication architecture is a blueprint of one of the Model County project's greatest assets: data. A well-defined data publication architecture helps to ensure that this asset is of the highest quality, is easy to access, and is as inexpensive as possible to maintain. The Model County vision for the publication architecture is to ensure that PROTECT data[4] is consistent and readily accessible for Model County justice partners. APPENDIX E provides the Publication Architecture Packet and additional detailed specifications. The overall context of the publication architecture is based on the desire to utilize existing repository information wherever possible to maximize data accuracy across the Model County environment. This is achieved by providing operational access to PROTECT information to non-PROTECT users. This context guides the state toward a distributed information-sharing topology that relies on the entire enterprise to maintain the quality and timeliness of the information available to Model County systems while at the same benefiting from the access to that information.

C. INTEGRATION ARCHITECTURE

The integration architecture provides the mechanisms through which Model County justice organizations and their partners are able to share information. This architecture will support the full range of information exchange, including Publish/Query, Push/Pull, and Subscription/Notification capabilities. This architecture is positioned to provide justice community access as well as appropriate nonjustice access, such as other government agencies (e.g., Children's Services), private sector businesses, and the general public at some point in the future. Although not currently planned, some of the nonjustice access may be on a fee-for-service basis.

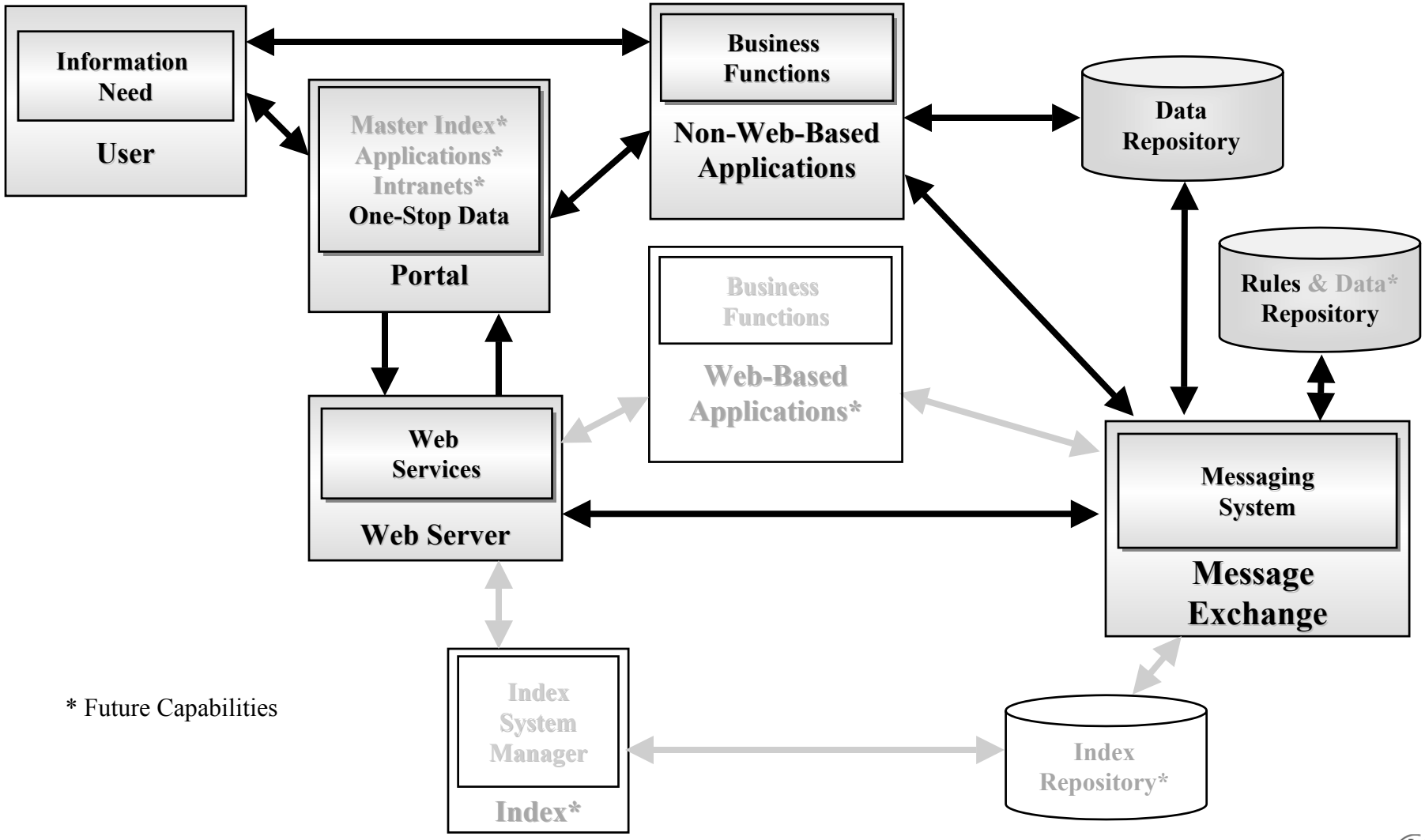
EXHIBIT VI-1, which follows this page, outlines the integration architecture for the Model County. The Model County integration environment illustrated in the exhibit includes a number of key components that rely on a robust network and security infrastructure (discussed in a subsequent section) and combine to deliver the desired integration functionality. The key components are:

- *User* – The user creates the information need in either real time or based on predefined requests that utilize the integration architecture. This represents the initiating activity or event that starts an information exchange within the Model County environment.
- *Portal* – The portal provides access to PROTECT data in the Model County environment. Although functionally complex, the portal is the tool that the Model County project will use to standardize and focus Model County application and information exchange efforts. Future

[4] The scope of the Model County project limits information publication to PROTECT data. This is the result of a number factors, including the narrow purpose of the grant that funded the Model County project.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

INTEGRATION ARCHITECTURE



* Future Capabilities

applications should be acquired and accessed through the portal, and existing applications should be extended to provide services via the portal. This provides a single maintenance point for changes to information delivery systems within the Model County environment.

- *Web Server* – The Web server controls the traffic allowed to access information through the Model County Web portal and temporarily stores requested information. It also provides fast access to critical information with the Model County environment.
- *Message Exchange* – The message exchange manages the information exchanges between justice organizations via the Model County information-sharing topology. Based upon preset business rules, this message exchange distributes Model County information to the Model County information-sharing topology and processes incoming requests from the Model County information-sharing topology for Model County information.
- *Rule Repository* – The role of the rule repository is to provide a maintainable storage platform for the complex business rules that will support the message exchange.
- *Non-Web-Based Applications* – Model County non-Web-based applications represent the existing application services that are implemented within the current partner organizations.

In addition, EXHIBIT VI-1 shows possible future expansions of the integration architecture. These are not within the scope of the Model County project but demonstrate that the design is intended to be extensible.

- *Rule and Data Repository* – The role of the rule and data repository is to continue to house rules, but to also fulfill queries from the Web portal without putting additional strain on the operational data stores. The data repository also provides the data resources to complex data research and analysis without affecting the operational systems.
- *Web-Based Applications* – Model County Web-based applications are common application services that could be implemented for local Model County partners that do not maintain their own systems. The Model County Web portal would act as the entry for these applications that provide basic functionality for organizations.
- *Index* – The index could store key components of the information contained in the data warehouse and operational data stores. This information could then be used to fill portal query requests, giving users a quick hit list from which additional information may be sought. In addition to the select information components, the index server could contain the location in the data warehouse, or data store, where the complete information is stored.
- *Index Repository* – The role of the data warehouse is to fulfill queries from the Web portal by providing the index information and operational data store for the requested data. This feature would provide an immediate indication of whether the information is available and the link to the system that houses the information.

The Integration Architecture Packet presented in APPENDIX F provides additional design information as well as specific design packets for this architecture. These components of the Model County integration architecture facilitate both access to information and the exchange of that information between state and local organizations.

D. ANALYSIS ARCHITECTURE

The Analysis Architecture Packet provides a brief outline of analysis capabilities that are possible within the Model County project. No specific analysis features are planned; however, some of the management capabilities that are necessary to manage the environment create the opportunity for limited analysis. The Analysis Architecture Packet is presented in APPENDIX G.

VII. MANAGEMENT ARCHITECTURE

VII. MANAGEMENT ARCHITECTURE

Technology environments typically consist of significant investments in multiple heterogeneous systems. This common situation is also true in the Model County project. Therefore, it is important to employ the management structures necessary to ensure the appropriate benefit is being realized from these investments. The IT management and support layer of the technology architecture represents the technology management processes for the future information-sharing environment. These management components are discussed from a logical perspective (i.e., they do not necessarily suggest a physical structure). The implementation (i.e., movement from logical to physical) must be an integral part of implementing information sharing within the Model County project.

A. POLICY REQUIREMENTS

The areas of policies and procedures that address change management and ongoing support of the technology architecture include:

- Project planning and initiation.
- Project oversight.
- Quality assurance.
- Requirements management.
- Contract management.
- Configuration management.
- Release management.
- Application support.
- Disaster recovery.

Each of these areas is critical to effective implementation and support of the efforts necessary to realize the Model County vision, goals, and objectives. Most of the issues have been addressed, but establishing clear policies, accompanied by appropriate procedures, will facilitate project management, reporting, communication, implementation, and support. The level of detail with which these policies and procedures are supported in day-to-day practice will, to a large degree, influence the risks and long-term success of the project.

B. IT ORGANIZATION

The organization, roles, and responsibilities involved in the management and operation of IT resources will change over the next few years. The current staff who are available to support Model County activities, ongoing project efforts, and internal needs will not be sufficient as the Model County project is extended. In fact, as Model County implementation begins, the technical functions supporting the Model County and its evolution must concurrently adapt to refine technical skill sets required to support the Model County environment. The staff who are identified to provide programming and support will accomplish the implementation but cannot sustain a long-term effort to extend the environment.

The Model County IT support structure will be primarily organized to provide regular business day/hour support by the current project staff. As the Model County information-sharing topology is developed and deployed, a small team will need to provide the help desk support for after-hours callers on all Model County functions. Initially, this functional group may consist of individuals who are on-call; however, as demand and utilization increases, this group should evolve to a 24/7 operation. The group should also provide backup support for local Model County partner organizations, where available, that have single-depth positions with limited or no backup.

C. IT MANAGEMENT TOOLS

As the Model County project is implemented, it will be critical that the appropriate tools, accompanied by structured processes and procedures, are in place to manage the future environment. In addition, key elements of application, infrastructure, and organization performance must be measured in terms of how well the architecture and IT support functions are meeting the requirements of the justice community. APPENDIX H, the Management Architecture Packet, provides the overall structure of the tool sets that should be employed within the information-sharing environment and, perhaps, the WIJIS environment, where appropriate.

Acquiring these tools, training IT staff in the proper use of the tool set, and establishing structured procedures for the application and use of these tools will provide the support infrastructure for the technology architecture within the Model County project. As previously discussed within the technology principles subsection, the Model County technical subcommittee should formally adopt the specific tools that will be used for each of the above tasks. In some cases, this process may have already occurred within the state's standards. However, all technology support tools should be formalized with an action plan that lists purpose, performance goals, tools, measurements, and actions to be taken when monitoring reveals performance issues.

In support of this point, APPENDIX H-1, the Security and User Database Design Packet, and APPENDIX H-2, the Auditing and Logging System Design Packet, provide the design parameters for two of the management support tools. These areas represent key features that are essential to the environment and must be deployed with the Model County project implementation.

APPENDIX A
GLOSSARY

GLOSSARY

Acronym	Definition
AAMVA	American Association of Motor Vehicle Administrators
CCAP	Circuit Court Automation Program
CIB	Crime Information Bureau
CJIS	Criminal Justice Information System
COTS	Commercial Off-the-Shelf
DA	District Attorney
DEG	Department of Electronic Government
DMZ	Demilitarized Zone
IAFIS	Integrated Automated Fingerprint Identification System
IT	Information Technology
JIEM	Justice Information Exchange Model
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MOM	Message Oriented Middleware
NCIC	National Crime Information Center
NGA	National Governors' Association
NIST	National Institute of Standards and Technology
NLETS	National Law Enforcement Telecommunication System
PKI	Public Key Infrastructure
PROTECT	PROsecutor Technology for Case Tracking
RMS	Records Management System
SOAP	Simple Object Access Protocol
STEP	Simple Transaction Exchange Protocol
TCO	Total Cost of Ownership
UDDI	Universal Description, Discovery, and Integration
VPN	Virtual Private Network
WAN	Wide Area Network
WDAA	Wisconsin District Attorney Association
WIJIS	Wisconsin Justice Information Sharing
WSDL	Web Service Description Language
XML	eXtensible Markup Language

APPENDIX B
BIBLIOGRAPHY

BIBLIOGRAPHY

International Association of Chiefs of Police, *Information Integration Planning Model*, April 2000, *http://www.theiacp.org* and *http://www.iacptechnology.org*.

Iyer, Jayanthi, WIJIS Model County Project, *Objectives and Deliverables Document*, Madison, Wisconsin, December 6, 2001.

Scribner, Ken and Stiver, Mark, *Applied SOAP: Implementing .NET XML Web Services*, Sams, January 15, 2001.

SEARCH, The National Consortium for Justice Information and Statistics, *Integration in the Context of Justice Information Systems: A Common Understanding*, Sacramento, California, April 2000, *http://www.search.org.*

SEARCH, The National Consortium for Justice Information and Statistics, *Planning for Integration: Developing Justice Information Exchange Points*, Sacramento, California, March 2000, *http://www.search.org.*

State of Wisconsin, CCAP STEP MOM, Madison, Wisconsin, June 21, 1999.

State of Wisconsin, Department of Electronic Government, *Sixth Annual Report of the Bureau of Justice Information Systems*, Madison, Wisconsin, March 2002.

State of Wisconsin, IJIS SOAP Messaging Project, *An Overview of SOAP*, Madison, Wisconsin, 2001.

State of Wisconsin, *The State of Wisconsin National Governors' Association Integrated Justice Information Proposal*, Madison, Wisconsin, August 3, 2001.

State of Wisconsin, WIJIS, *Model County Project Law Enforcement Interface*, Madison, Wisconsin, February 18, 2002 (Draft).

State of Wisconsin, *Initial Steps for Establishing a Statewide Integrated Justice System*, Madison, Wisconsin, October 4, 1995 (Draft).

Wiegers, Karl E., *Software Requirements*, Microsoft Press, Redmond, Washington, 1999.

APPENDIX C
INFRASTRUCTURE ARCHITECTURE PACKET

INFRASTRUCTURE ARCHITECTURE PACKET

Model County operations and management will be supported by a small array of computerized Web-based information-sharing services, which will run on server and security infrastructures. These key strategic assets must be managed to maintain their value and minimize their total cost of ownership (TCO). The technology architecture that supports the Model County's future vision will be based upon a set of infrastructure architectures that facilitate primary Model County business exchanges. The infrastructure architecture is represented by the vision below.

A. VISION

The infrastructure architecture will be largely based on the current infrastructure model, but will include additional features needed to support improved security, performance, and availability in the Model County environment. The need to use current systems and minimize additional infrastructure purchases is recognized as a critical success factor for the Model County. Although some new equipment will be necessary, every effort will be made to ensure funds are committed effectively.

B. PRINCIPLES

The components of the infrastructure layer consists of server infrastructures implemented within a few common principles and tactical decisions applied to the infrastructures. The following principles apply to the infrastructures in the target Model County infrastructure environment:

- Invest in Stable Technology

  The Model County project should purchase infrastructures and operating systems that are tested and have widespread acceptance by the IT industry. The Model County should avoid the absolute newest technologies unless the implementation and support risk can be clearly justified. Production systems should not rely on alpha and beta product releases.[1] The basis for all server decisions should be ensuring the highest quality of service to the end users. Trade-offs between the best performance and supportability need to be balanced and factored into long-term infrastructure decisions.

[1] Many IT support organizations have limited technical staff resources, and the Model County project does not have any support staff. Therefore, a prudent strategy is to wait to implement a new technology until at least the first patch is available for a production-level release to help ensure that first-release bugs and problems have been worked out by a large number of real-world users. There are some application needs within this architecture that may affect this principle.

- Avoid Obsolescence

  Defined infrastructure standards are not intended to force retirement or replacement of existing systems. Long-term plans and support costs must be considered when implementing new systems. Model County technology plans need to consider strategies for the removal of non-strategic or retired technologies. Procurement of retired technologies should be considered only as a stopgap measure.

- Implement Vendor-Neutral Solutions

  Vendor-neutral solutions should be applied whenever possible. Servers will be implemented as component-level tools, not to be coupled with, or dependent upon, proprietary vendor application offerings. Hardware vendors should be ISO 9002-compliant. However, application components may require certain operating systems.

- Use Common Manageability and Support Options

  Hardware and software should comply with industry standards for remote control and monitoring. Vendor and configuration considerations should include the availability of trained field support and the ability to accommodate upgrades.

- Implement Replacement Plan

  The Model County should have a server infrastructure replacement policy. System cascading should be employed to reuse older equipment where feasible and cost-effective. The Model County project team should develop a defined support cost limit to balance the value of old equipment and the cost of maintenance and support.

C. DESIGN DECISIONS

The following tactical decisions should apply to both the server environments and client systems within the Model County infrastructure environment.

- The Model County will establish an equipment area.

  All infrastructures in the Model County environment will be deployed in a location that has yet to be defined. The collection of the servers and equipment will be a specific group of systems that support the Model County and reside on a network that is physically separate

from the rest of the systems housed in the facility, wherever it is located. This is discussed in the Equipment Area Design Packet, APPENDIX C-2.

- Infrastructures will be chosen that have remote manageability.

  All infrastructures deployed in the Model County environment will have secured remote management capability. This applies at the server level in support and operations and at the client level with the ability to update and maintain any end-user devices supported by the Model County environment.

- Infrastructure support will be Web-based.

  This will allow the remote manageability necessary across the Model County environment. In addition, it allows the support staff to primarily utilize the same environment that the Model County staff utilize.

- Server devices will be selected with common infrastructures.

  Infrastructures will be selected that utilize common or similar components. This will allow Model County support staff to maintain a small, common replacement part pool that may be used to rapidly repair devices. In addition, similar operating systems and software drivers will enable Model County staff to simplify maintenance efforts. The commonality will focus on all possible components of the infrastructure design.

These decisions will focus the infrastructure efforts into common approaches that support the Model County.

D. DISCUSSION NOTES

The following discussion notes should be considered in support of the information presented in the previous subsections:

- The Model County equipment area may seem redundant; however, specific security and access requirements that organizations must comply with to access federal systems, such as National Law Enforcement Telecommunication System (NLETS) and National Crime Information Center (NCIC), are easier to validate and manage in a separate topology. This does not mean that these systems have to reside in an isolated building; however, specific access and management procedures and rules must be established.

E. INFRASTRUCTURE DESIGN PACKETS

The architecture and associated design packets support the infrastructure architecture by highlighting specific points that meet the needs identified in the Model County Business Requirements document. Three aspects of the infrastructure layer require additional design detail and are developed in the following subappendices as design packets. Specific design packets for the infrastructure architecture packets are:

- *Information-Sharing Topology (APPENDIX C-1)*. This design packet identifies the physical design topology of the servers and computing equipment that support the Model County information-sharing functions. The devices are also described in this design.
- *Equipment Area (APPENDIX C-2).* This packet outlines equipment area design principles and decisions. The area that houses and operates the servers is essentially a mini-data center. To minimize confusion and the impression that this is a large, complex facility, this area is referred to as the WIJIS equipment area. It is a few racks of equipment that provide the computing power and security devices for the Model County. This design packet identifies the design elements of the equipment area.
- *Security Architecture (APPENDIX C-3).* This design packet outlines tactical security design principles and decisions. The security architecture provides the design for the security systems that will be used to securely connect to the equipment area and the services provided on that equipment.

The current infrastructure and systems will continue to provide the operational support for Model County partners. In addition, hardware consisting of servers and security devices will be necessary to create the environment needed to share information in Wisconsin. This collection of devices must be housed and supported in a facility that has not yet been determined; however, the equipment and its location have been referred to as the information-sharing topology.

INFORMATION-SHARING TOPOLOGY DESIGN PACKET

This subappendix provides the design view of the servers that should be used to support the Model County application and Web site environment. The infrastructure that supports the Model County environment is critical to the Model County's success. The design model establishes the criteria for the technical system infrastructure that provides the environment's application services. The vision of the system infrastructure is outlined below.

A. VISION

The vision of the information-sharing topology is to create a common service that can be used by all Model County partners. The topology will be located in the equipment area detailed in the next design packet and focuses on providing the necessary Web services, message exchange and management features, and query capabilities to meet the business requirements outlined in the Business Requirements document and in the parallel design packets in this Technology Architecture. This vision is supported by the principles outlined in the next subsection.

B. PRINCIPLES

The important design principles that affect the server model are listed below.

- Primary Exchange Platform

  The information-sharing topology will be the primary means to exchange data within the Model County project. The majority of criminal justice and public safety information exchanges that are being modeled with the Justice Information Exchange Model (JIEM) tools will be developed in this environment.

- One-to-Many Interface

  Systems will have one interface to the information-sharing topology that will be used for all information exchanges. This design principle promotes the use of a single information feed from existing systems to accomplish all information movement to and from those systems. This is a critical design point to minimize maintenance and allow the development of future features within the Model County technology architecture.

- Data Transformation Responsibility

  Data transformations, if required, will be the responsibility of the information-sharing topology. This principle focuses the work required to make data and information fit the receiving system-specific specifications on the rule-based environment that supports the movement of information. The key point is that activity may benefit other exchanges that have not been implemented and will reduce to the number of places the business logic must be maintained.

These principles guide the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The design decisions guide the information-sharing topology. These decisions will be used to structure the implementation characteristics of the topology. Topology choices will support the overall environment outlined by these design guidelines.

- The Model County project will use Microsoft SQL Server and BizTalk to implement the information-sharing topology.
- Implementations and XML, SOAP, WSDL, and security specifications will follow industry-standard, not Microsoft-specific, formats.
- The central design will be based on an n-tiered design consisting of application (Web-based) services supported by transaction services connected to the data repositories.
- Every effort will be made to compartmentalize design elements so that specific maintenance efforts are conducted at the discrete element level.

The information-sharing topology will have several impacts on the specific design of component systems. These impacts are described in the discussion notes below.

D. DISCUSSION NOTES

The information-sharing topology issues that must be managed are primarily centered on the ability to support the environment. The specific issues that must be managed are outlined below.

- The n-tiered approach will require significant staff expertise that must be factored into the transitions from vendor services to Model County-provided services.

- The information-sharing topology offers the Model County the opportunity to design components in modular format that will take advantage of the centralized infrastructure. Specifically, Model County information exchanges should be based upon components built within the central transaction environment, not in the database or application layers. This modular approach will allow all of the Model County and partner applications that use that particular function to return the same information to all calling applications.
- It is important to realize the benefit offered by the design approach. The primary benefit of the information-sharing topology is that the ability to support the application environment is significantly enhanced by the control and central maintenance of exchanges that are offered by the transaction approach. Additional benefit will be derived from a reduction in the number of technical skills necessary to support the various systems. This reduction is a result of the need for common skills, not system-specific skills.

EQUIPMENT AREA DESIGN PACKET

This subappendix provides the design view of the equipment area that should be used to support the Model County servers and equipment. This design model establishes the criteria for the technical system infrastructure that houses the environment's application services. The vision of the equipment area is outlined below.

A. VISION

The vision of the equipment area focuses on two primary zones that serve specific purposes for the application services. EXHIBIT C-2-1, which follows this page, depicts the structure of the equipment area model. This model consists of a demilitarized zone (DMZ) and a server zone. Specific design elements of this vision are listed below.

- The DMZ will contain the Web servers that provide the actual services to the user community.
- The server zone will house the primary non-Web servers and data repository servers.
- The equipment area will be based on a key, high-availability database server, application server, and message server, as well as key Web servers configured in a farm arrangement to support both high reliability and Web service compartmentalization.
- A central site that has the capability and reliability to support the technology will provide the support and management for this infrastructure.

The equipment area vision is supported by the principles outlined in the next subsection.

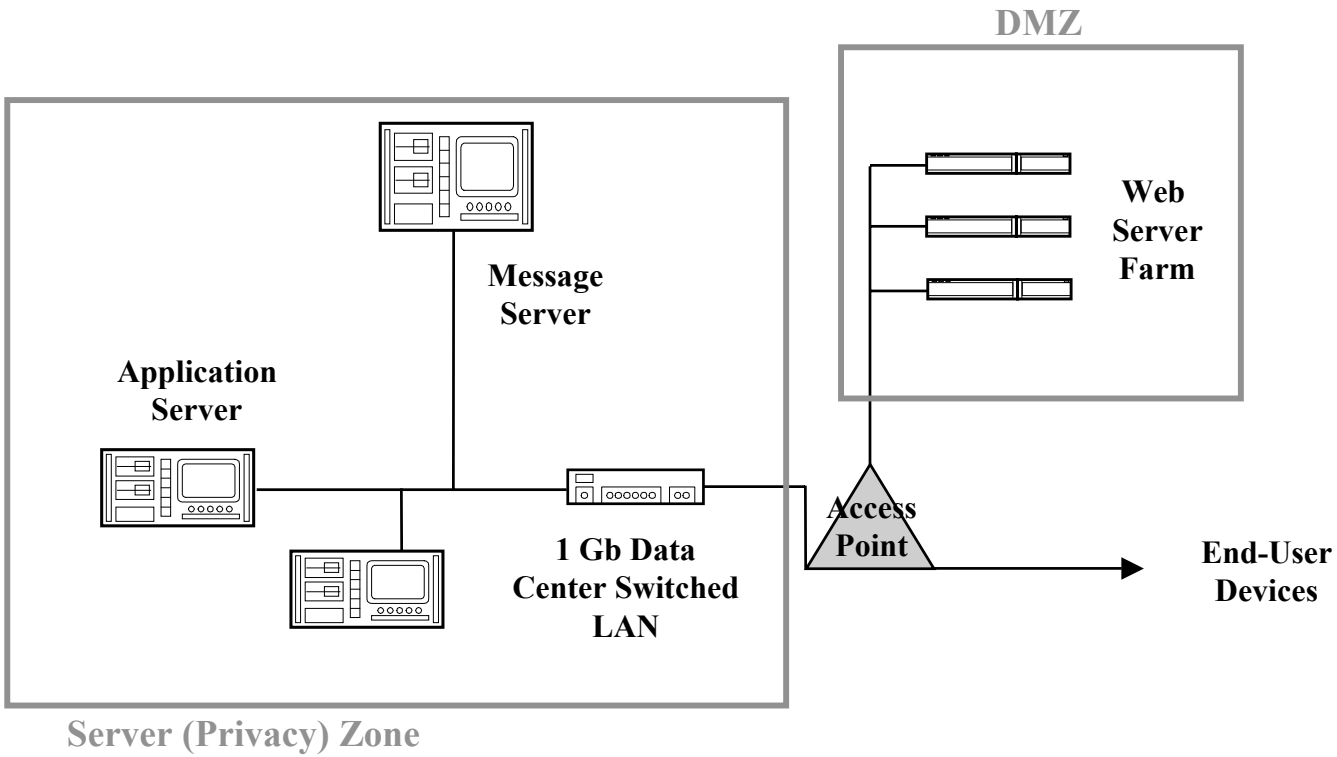
B. PRINCIPLES

The important design principles that affect the equipment area are listed below.

- Database instances will be aggregated on a single server. This does not preclude the existence of several databases on the single set of hardware.
- The Web servers will provide multiple Web sites to allow for ease of security and performance configurations.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

EQUIPMENT AREA MODEL



NOTE: This model depicts primary data center device types only.

- The primary network structure will be a 1 Gb or greater local area network (LAN) that supports the server zone.
- If feasible, the server zone should include a redundant 100 Mb or greater LAN that can provide immediate primary LAN fail-over.
- Servers should be internally redundant wherever possible.
- Servers should be configured with multiple support and network paths wherever possible.
- Server interfaces should be established with a switched 1 Gb Ethernet or greater LAN.

The principles support the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The design decisions guide the equipment area model. These decisions will be used to structure the physical implementation characteristics of the equipment area devices and topology. All construction and implementation choices will support the overall environment outlined by these guidelines.

- Only Model County-specific systems will be housed in the Model County equipment area.
- Device utilization should not exceed 70 percent for any sustained period.
- Performance monitoring of all components will be done regularly to ensure effective operations.
- The application environment will be housed in the equipment area and will be supported by Model County project staff.
- Servers will be structured to support technical aspects of the environment, not specific application structures.

A consolidated Model County equipment area will have several impacts on the specific design of component systems. These impacts are described in the discussion notes below.

D. DISCUSSION NOTES

The equipment area model issues that must be managed are primarily centered on the ability to support the environment. The specific issues that must be managed are outlined below.

- The network structures that operate the equipment area must be correctly tuned and continuously monitored to ensure that back-end processes do not choke out end-user communication.
- The equipment area must be established to support multiple calling applications and systems.
- A significant benefit is the ability to implement new functionality based on existing components within the equipment area through the use of existing servers that are already tested and operational. These benefits will yield improvements to the entire Model County environment.

SECURITY ARCHITECTURE DESIGN PACKET

This subappendix provides the design view of the security environment that should be used to support the Model County. The security components that support the Model County environment are critical to the Model County's success. This design model establishes the criteria for the technical security infrastructure that provides the environment's security services. The vision of the security design is outlined below.

A. VISION

The vision of the security infrastructure is to provide a robust and manageable security environment that meets or exceeds the requirements of the Model County. Security will include:

- The definition of end-to-end security standards and architecture.
- Implementation of security at the network, system, database, and application levels.
- Implementation of appropriate security processes and procedures.
- Clear roles and responsibilities regarding security management.

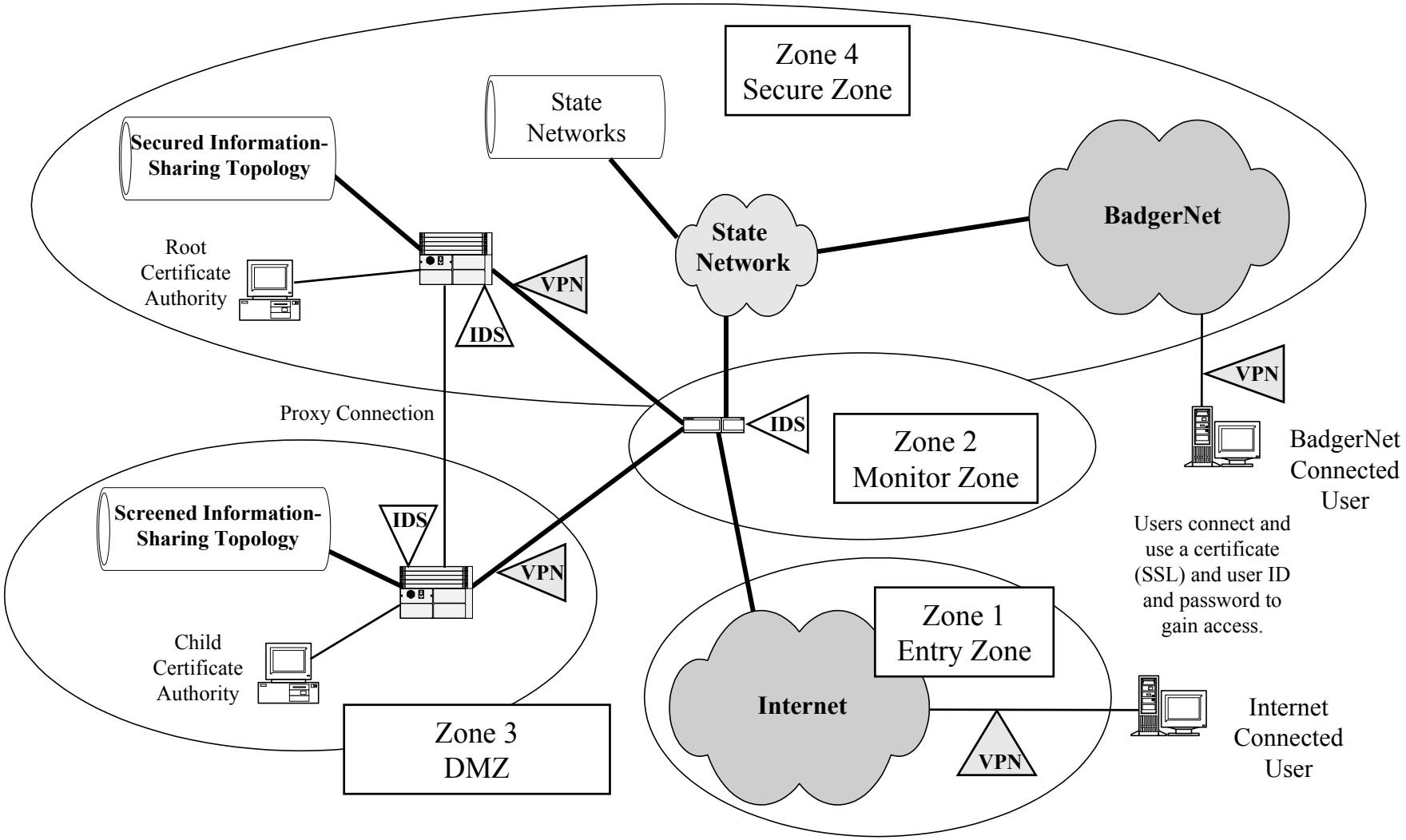
The security architecture builds upon the proposed network and hardware infrastructure. With the open exchange of Model County information, it is critical that the information be protected. The primary components of the security architecture are VPN, firewalls, intrusion detection, proxy servers, and digital certificates.

B. PRINCIPLES

As justice agencies take advantage of an Internet/intranet-based work environment, mobile computing, and other advancing technologies, addressing associated security considerations and requirements becomes increasingly important. Serious attention must be given to the security needs of agencies in this environment. The security architecture is framed and defined through the policy framework, tactical decisions, and functional design outlined in this subsection. Thus, the technology security architecture helps further define security requirements and frame the development of solutions. EXHIBIT C-3-1, which follows this page, highlights the components of the security architecture. The architecture builds upon four primary security zones as described below.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

CONCEPTUAL SECURITY DESIGN



- *Zone 1 – Entry Zone*. The purpose of the entry zone is to utilize the entrance router and firewall to control physical access into and out of the network.
- *Zone 2 – Monitor Zone*. The purpose of the monitor zone is to watch the network traffic at the critical branch structure between networks.
- *Zone 3 – DMZ*. The DMZ provides a secured area to place devices that will be exposed to open network traffic and have a higher risk of compromise.
- *Zone 4 – Secure Zone*. This zone provides the area to place all server devices that require increased security and protection.

This architecture is based on several assumptions about the relationship between the security structure proposed in this document.

- The proposed security architecture is based on a number of basic security requirements that comply with the Model County security standards.
- An internal security audit will be performed to identify security risks and recommend specific actions to validate, refine, and address detailed security policies and procedures.
- The technology security architecture for the Model County will be updated as a result of the security audit, as appropriate.

The following security principles will be applied within the Model County architecture and, if necessary, the Model County will need to revamp existing security policies and procedures to adequately implement security and meet the needs of the justice community. These security principles will evolve and expand through completion of the projects in the Model County implementation plan. However, it is anticipated that the following policy framework will be adopted:

- Controlled Physical Access

  Security policies and practices will control physical access to Model County technology resources. These controls will likely include:

  - » Equipment area access controls that manage, track, and control the individuals who have access to equipment area resources.
  - » End-user device controls that enable the Model County to manage, track, and control the devices that have access to Model County technology resources.

» Device authentication that allows strict authentication for access to highly secure resources and little or no authentication requirements for access to other applications and information.

» Device location controls that enable the Model County to control the network access points from which a physical device may access applications and information.

- User Access Controls

  Any individual accessing a system will be uniquely identified. All access will be controlled through common user account databases that maintain consistent management guidelines and audit functions. User authentication will be employed, and the authentication method will likely vary depending on the security requirements of the application and information being accessed.

- Access and Data Activity Logging

  All session initiations, session terminations, failed access attempts, and access violations will be automatically logged. Data activity logging will be initiated whenever feasible. Centralized auditing and management of this information will be done by the state, although the physical activity may occur in the application support area.

- Data Encryption

  All sensitive data passing over public network segments or otherwise open networks will be encrypted to ensure privacy, authentication, and nonrepudiation.

- Intrusion Detection

  The state will actively employ intrusion detection practices to monitor activity and automatically identify and react to intrusions into Model County resources.

- Regulatory Audits

  System audits will be performed regularly to verify system configurations and expected system usage patterns. This will be done to ensure that the correct levels of accessibility are being applied to enable the appropriate job function and, conversely, to ensure that information is not available to inappropriate personnel.

- Other Detailed Policies and Procedures

  Other detailed security policies and procedures will be established to manage situational concerns such as:

  - » Remote access points and usage.
  - » Password structure and aging.
  - » Systems administration rights.
  - » New hire and exit criteria.
  - » Access control, logistics.
  - » Certificate usage and expiration.
  - » Intrusion criteria.
  - » Security compromise notifications.

This policy framework, when implemented in practice, will provide the level of security necessary to safeguard the private and confidential information maintained within the justice community. Security repository design will be discussed in APPENDIX H-1, the Security and User Database Design Packet.

C. DESIGN DECISIONS

This technology security architecture is based on key design decisions about the requirements detailed above and the likely solutions that will be used for the Model County. The context of the security decisions are based in four areas:

- *Confidentiality* – Information is disclosed only to users authorized to access it.
- *Integrity* – Information is modified by authorized users and only in approved ways.
- *Availability* – Use of systems cannot be maliciously denied to authorized users.
- *Accountability* – Users are accountable for their security-related actions.

These decisions are described below and are followed by a discussion of the functional design for hardware and software that will be employed under this architecture.

- Support Statewide Justice Security

  Many Model County applications provide shared services to the Model County community, and this is a role that the Model County is very likely to perform well into the future. Because of this, the Model County security design must fully consider securing the access to these resources by other state agencies, local agencies, state and local nonjustice agencies, private service and legal firms, citizens, and other entities. The security services provided under this design will extend to external constituents.

- Support Wide Area Network (WAN) and LAN Access

  Current access to the Model County applications by external entities is largely through either dedicated devices or closed systems. Model County application services will be provided to agencies through the Internet, WANs, and LANs. These networks may be open and support nonjustice personnel. The technology security architecture must be robust in its support of this type of operating environment.

- Support Remote and Mobile Access

  There has long been a demand for access to justice information and applications in the field. Technology advancements have made delivery of this information and applications feasible. The technology security architecture must be robust in its support of this type of operating environment.

- Use Industry-Standard Technology

  The Model County is not chartered or funded to research and develop custom technology security solutions. Because of this, the state will rely on industry-standard technology security mechanisms.

- Comply With Mandates

  The Model County participates in a number of federal and national organizations that share the use of applications and networks. In doing so, the state must adhere to the security policies for those applications and networks. The Model County technology security architecture should support these requirements.

- Refine Security Plans and Policies

  In conjunction with the Model County-sponsored security audit, the state should refine security policies and procedures for all of its applications and networks once the final recommendations are received.

EXHIBIT C-3-1 identified several physical components of the security architecture that are already in place. The discussion notes below provide additional comments on the security design.

D. DISCUSSION NOTES

The technology security architecture builds on the future network and hardware infrastructure architectures previously described. The security functional architecture includes the following key components:

- Firewall technologies.
- Intrusion detection.
- Directory server.
- Web servers.
- Certificate authority.
- Authentication server.
- Client-side encryption software.

The specific implementation of these components will be detailed in the Technology Specifications document.

APPENDIX D
APPLICATION ARCHITECTURE PACKET

APPLICATION ARCHITECTURE PACKET

Local and state criminal justice process operations and management are, and will be, supported by an array of computerized applications. These applications are key strategic assets to the Model County project and must be managed to maintain their value and to minimize their TCO. In addition, the Model County project will provide additional application components in a Web format that also need to be maintained and consistent with the environment. The current applications and the Model County components comprise an application architecture that is discussed in more detail below.

A. VISION

The application architecture components are a focal effort in implementing the Model County technology architecture. The application architecture represents the Web-based functionality that will enhance the environment and support information exchanges. These components will support operations of the justice organizations and transfer the data needed for Model County information exchanges. The lessons learned from the Model County application architecture will guide future efforts.

B. PRINCIPLES

To manage these assets effectively, the Model County project will apply the core technology principles discussed in Section IV of the main document to:

- The manner in which these components will be developed and maintained.
- The relationship between these components.
- The built-in ability to support and manage these components.

Applying the core technology principles within this framework means that the project will create an environment that exhibits the following design principles:

- Provide Ease-of-Use

  Components will be characterized by technical structures that facilitate ease-of-use and enhance justice staff efforts to accomplish daily tasks. Ease-of-use is user-focused, although effort should be given to the ability to technically reuse all components.

- Minimize Maintenance Requirements

  Required support efforts for the systems, information access, and interchanges will be minimized to help ensure efficient use of limited technical resources. Development of any component will include built-in maintenance features to make the component extensible and maintainable. This is a critical design principle, given the size of technology support organizations and current funding trends.

- Support Information Conversion Within the Environment

  The resulting use of the components will create or modify information within the system so that disparate systems can have access to the same information feed with the necessity to modify core systems. This feature is only required where the information format is not accepted by the core system. It is important to have the ability to modify the information at the exchange point so that the systems do not have to be extensively modified.

These principles guide the manner in which components and any Web applications will be developed. The design decisions provided in the next subsection reflect that guidance.

C. DESIGN DECISIONS

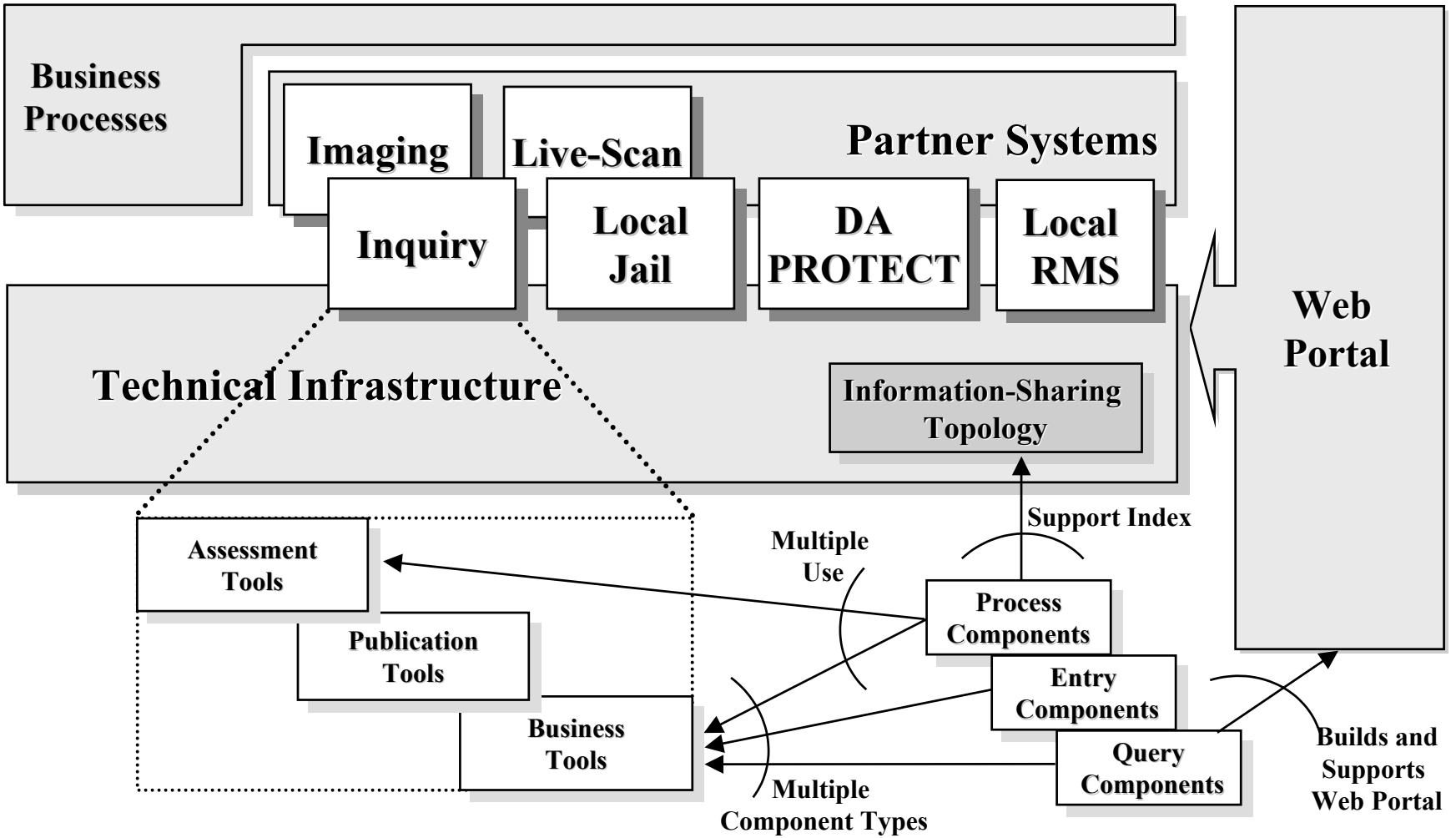
The application architecture and goals outlined above are further refined and focused based on a series of design decisions that support the core technology principles and architectural qualities for the Model County information-sharing topology and applications. The tactical decisions are:

- Develop Discreet Components

  The Model County project will develop the technology architecture in component groups. EXHIBIT D-1, which follows this page, depicts the functional groupings for components. This design provides a logical method to develop and test specifically focused components that can then be aggregated as a whole within the integration and application environments. The complex matrix of types of components provide specific functions within the environment. The combination of these components create various application tools that provide different types of capabilities, depending on the combination. The Model County project will primarily focus on publication and business tools that support information access and sharing.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

APPLICATION DESIGN MODEL



- Support Evolutionary Change

  The Model County project will develop an implementation road map that supports the gradual addition of components to the technology architecture. This evolution will be based on implementing publishing solutions, implementing Model County integration components and, finally, developing and enhancing a messaging solution. The overall objective of these changes is to increase the amount of accurate information made available to justice staff in a timely manner for Model County partners.

- Adopt Internet Architecture

  The Model County project will adopt an Internet-based architecture for all applications components. Application configuration decisions should be based on the n-tiered technologies envisioned in the infrastructure architecture (APPENDIX C). Separating application graphical user interface, logic, data, and their associated processing and maintenance systems will improve application integration management, both locally and remotely.

- Use Standardized Development Tools

  The Model County will adopt an industry-standard set of application development tools and databases and expand or refine the current standards to embrace state justice integration standards as well as the needed new standards to support the technology environment. Vendor-neutral standards should be applied whenever possible to allow for reduced system integration and maintenance efforts. By decreasing the variability and complexity of application-related tool sets, the Model County project can take full advantage of standardized application and technology offerings without having to acquire unique, specialized skills for individual components.

- Buy, Not Build

  The project's preference is to buy, not build, application and platform architectures wherever possible. It will purchase applications that are tested and generally accepted by the IT industry. Existing facilities will be leveraged to achieve application goals where possible. Ensuring the highest quality of service to end users needs to be the basis for all technology decisions. Trade-offs between the best performance and the TCO need to be balanced and factored into long-term platform decisions.

The decisions highlighted above provide overall design guidance to the application layer of the integration model. Specific design packets for the application architecture packet are:

- *Web Site Design Packet (APPENDIX D-1).* This packet presents the tactical principles and decisions that guide Web site and component design.

The design packet supports the application architecture by highlighting specific points that meet the requirements identified in the Business Requirements document.

D. DISCUSSION NOTES

The following discussion note should be considered in support of the information presented in the previous subsections:

- Web Portal

  Although discussed in APPENDIX F, the Integration Architecture Packet, the Web portal represents a single, Web-based access point to the systems and information contained within the Model County environment. Therefore, all application efforts should consider requirements outlined in the Integration Architecture Packet. In addition, the Web portal contains a security and authorization layer that tailors the available options to match a user's security profile; these features are detailed in APPENDIX H, the Management Architecture Packet. This affects the design of all applications in this architecture packet and subsequent supporting design packets.

WEB SITE DESIGN PACKET

This packet provides the Web site design principles that will be used to access all Model County applications, features, and support systems. The central concept of the Web site is that a user should need to use minimal clicks to accomplish an action. The vision, principles, design decisions, and discussion notes listed below provide the guidance for the conceptual design of all Model County Web sites. The vision of "single-click" access is described in the next subsection.

A. VISION

The vision for the Web site design is summarized by a rapid, secured access method to the primary business functions desired by the user. Although these features are minimal for the Model County, this access will provide the major functional areas grouped by access category. It will also have the ability to get to all information as needed. EXHIBIT D-1-1, which follows this page, depicts a model Web design. Additional components of the vision are listed below.

- The Web site will consist of functional areas covering specific organizations (such as WDAA or local law enforcement, Model County [WIJIS], and a non-WIJIS user communities).[1]
- Within each functional area, specific application services (inquiry features) will exist.
- Application services will exist in only one functional area. Organization users will have access to all three functional areas. Model County (WIJIS) users will have access to the Model County (WIJIS) and non-WIJIS areas. Non-WIJIS users will have access only to non-WIJIS areas.
- The focus of each page will be a single-click access point for each type of user.

The Web site vision is supported by the principles outlined in the next subsection.

B. PRINCIPLES

The Web site should provide clear, focused access to application functions and information for an organization's staff and customers. The central principle is that the Web sites will follow

[1] The non-WIJIS user communities are not built at this time; however, this design should incorporate the features to avoid significant rework in the future. This area may initially house maintenance and monitoring features.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

WEB DESIGN MODEL

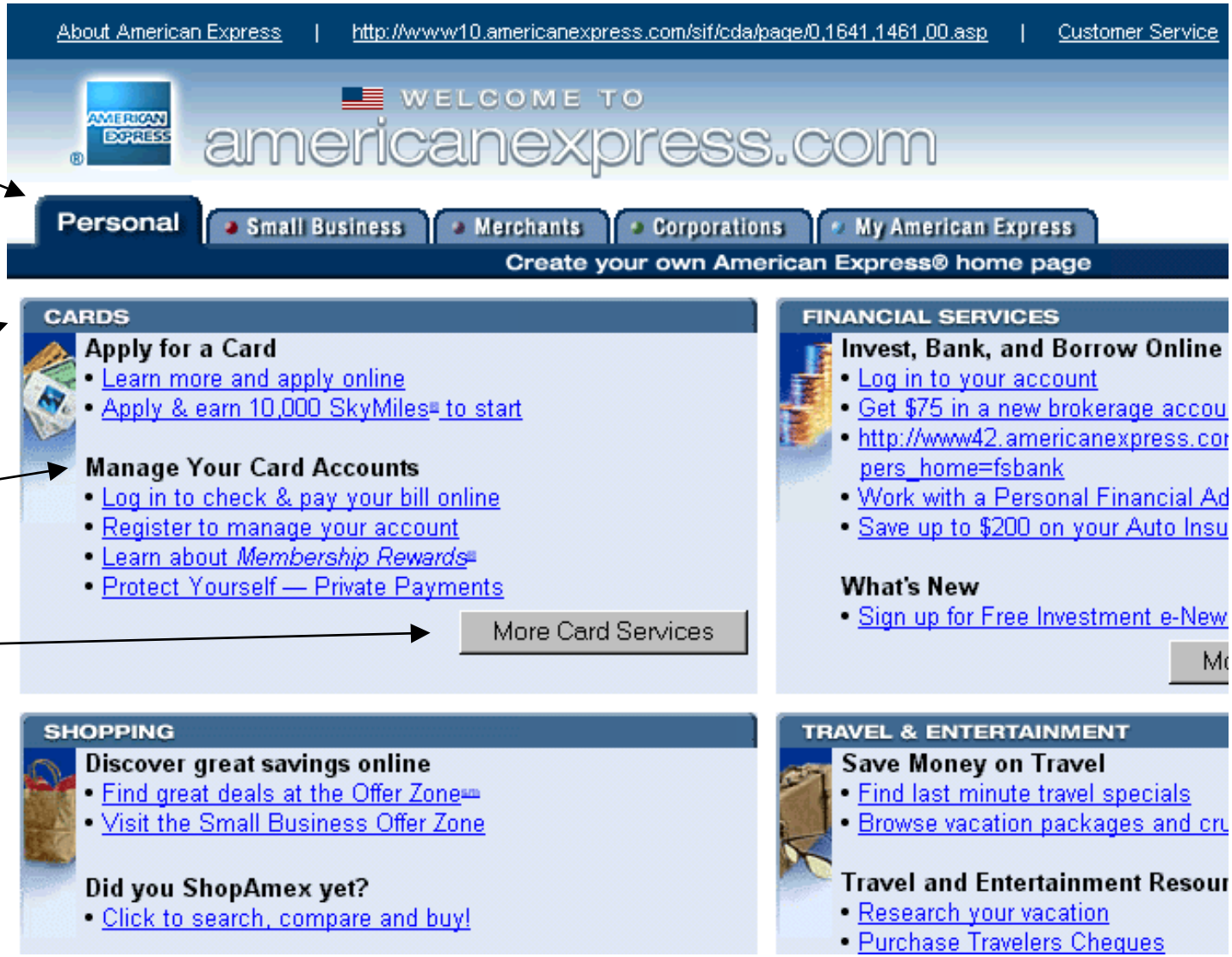
Key Design Elements

Major Functional Group Tab

Major Functional Area

Major Services (Organized by Category)

Additional Function Link



fundamental design principles published by the project team and DEG. In addition, the following principles will be incorporated into the project's existing design principles:

- The Web site will provide content for the entire enterprise, although users will only see authorized access points.
- Functional areas will be tab-based and will provide the options to all users of that level of services.
- Within each access point, users will only see the functional areas that they are authorized to access.
- Users will not be able to see a service within a functional area when they are not authorized to access that particular service.
- A common set of standards will be defined for the Web interface.
- Web services will be implemented in a redundant method consistent with DEG and WIJIS standards.
- The site layout will support access to primary functional area services in one click.

The critical behavior is that the Web sites will be constructed to provide single-click access. EXHIBIT D-1-1 shows an extract from *http://www.americanexpress.com* and is a good example of the single-click approach. This site organizes applications and functions into functional groups, functional areas, categories, and finally services. This organization approach is critical to providing access in a single click. These principles are supported by the design decisions in the next subsection.

C. DESIGN DECISIONS

The tactical design decisions guide the construction and implementation of Model County Web sites. These decisions will be used to structure the physical implementation characteristics of the actual Web pages. All construction and implementation choices will support the single-click vision outlined by the following:

- There will be three primary tabs (functional groups) on the Web page: General Services, WIJIS Services, and Organization Services (Agency/Organization tab such as WDAA, local law enforcement, etc.).
- Each tab will offer specific application service areas (functional areas) that will list the primary functions of the application.

- Specific application service areas will group the services provided into logical categories, listing each of the offered services.
- When a service is selected, the Web site will hand off authentication information to the application service.
- A user will only be able to see the functional areas, categories, and services that they are authorized to access.

The design decisions are key concepts that must be clear to all developers and vendors for a consistent look and feel within Model County applications. The next section outlines discussion notes related Web site design.

D. DISCUSSION NOTES

The following discussion note outlines tactical issues that must be managed:

- Standardization of the Web pages so that a common look and feel is maintained throughout the environment. The specific issues that must be managed are outlined below.
  - » Retrofitting existing Web-based services to the new common standards will involve an undefined, but not substantial, effort.
  - » Application of the standards and approach within all of the Web pages in the environment must be prioritized to simplify the environment for users.
  - » The dynamic display features of the Web site require a clearly defined user authority database as well as tight integration with the Web services.

In addition to these issues, it is important to note that the single-click approach will yield significant improvement in the usability of Model County services, as well as the satisfaction with and support for those services.

APPENDIX E
PUBLICATION ARCHITECTURE PACKET

PUBLICATION ARCHITECTURE PACKET

Data design is the process of conceptually modeling data in a manner that will maximize data integrity, availability, and shareability while minimizing administration and maintenance. The conceptual data design must be sure to support Model County business functions. While the architectural design issues presented in this appendix create a complex matrix of considerations for the Model County environment, adherence to the principles and design will minimize future implementation issues.

A. VISION

The data design should present an overall conceptual vision that shows the major data stores that will be used and the relationships between these data stores. This design will be used to guide Model County component development and enhancements. Key concepts within the publication vision include:

- Lookup components will be used to retrieve information from each individual data store as needed to support publication queries.
- The design for the PROTECT lookup can be extended to other systems, provided that additional supporting components are added.
- Design features will be clearly documented and available electronically to provide rapid troubleshooting in the event of problems.

The publication vision is supported by the principles outlined in the next subsection.

B. PRINCIPLES

Several key design principles guide the publication design. These principles provide the design rationale that will be used to determine design choices during system creation and implementation.

- Defined XML Formats

  XML definitions for each exchange will be maintained for consistency and planning purposes. Updates to the definitions will be made for new data elements that are necessary based on any new data set or redefinition of the XML document. This type of update should be based on SOAP/XML format to update the definition.

- Vendor Offerings

  The readily available and most robust vendor applications addressing Model County requirements have data structures that are relatively similar from vendor to vendor. The conceptual common structures should match these constructs. Within the context of the Model County, these will be the Spillman systems (Green Lake). These should be balanced with the national standards for the purpose of extended this solution beyond the Model County.

- Maintenance Effort

  The publication model should be designed to minimize the database administration, given all other factors. In addition, the data exchange mechanisms, i.e., SOAP messages, will be built in a modular architecture so that databases can be maintained and enhanced independently.

These principles are supported by the decisions in the next subsection.

C. DESIGN DECISIONS

The following publication architecture decisions have been established to guide the strategic management of data in terms of a well-structured, meaningful plan for the deployment, use, and protection of business-critical information.

- Support Diverse Data Types

  Justice operations involve the gathering and evaluation of information (e.g., evidence) from a variety of sources, often in a variety of forms: paper, images, audio, video, and electronic. If Model County partner applications are to match and effectively support its business practices, these applications must be able to capture, store, organize, retrieve, and present all these different types of data. As a result, the Model County will invest in technology that provides the ability to use these resources.

- Allow Some Data Redundancy, if Required

  Traditionally, data redundancy has been avoided to maximize the use of expensive data storage facilities and to minimize data complexity. Today, with the onset of inexpensive storage, some data redundancy issues are not as critical as they once were. While the state will strive to avoid the development of redundant data-handling processes, it will cautiously accept a degree of data redundancy if required to address a business need.

- Follow Existing Data and Exchange Standards

  Many standards have been established to guide the format and exchange of Model County-related justice information. Existing data standards include those determined by the state, NCIC, American Association of Motor Vehicle Administrators (AAMVA), National Institute of Standards and Technology (NIST), and others. Unless there is a compelling reason to depart from the established standards, the Model County should continue to observe them. In choosing standards, the state should follow a decision tree:

  » Is there a federally or nationally mandated standard set forth in the subject area served? One example is the Electronic Fingerprint Transmission Specification established by the FBI for the submission of arrest fingerprints.

  » Are there other applicable standards (e.g., NCIC, AAMVA, NIST)?

  » Is there a standard defined in the state standards?

  » Is there a leading or emerging standard in the IT industry?

  » What standards do the market-leading-solution provider use?

  » Is there another regional or local standard?

- Invest in XML and SOAP

  Given the vision of moving to a browser-based environment, it is important accept the emerging technologies that will drive the environment into the future. XML and SOAP, the emerging standards for the exchange of data over the Internet, can facilitate the creation and distribution of a wide variety of information objects and or documents. There are a number of mandated standards for data exchange in the justice community (e.g., NCIC and IAFIS are well established). Where no specific XML or SOAP exchange standards are mandated, the Model County project will use XML methods and structures to support data exchanges between programs and agencies.

The decisions highlighted above provide overall design guidance to the information component of the publication layer of the integration model. The specific design packet for the publication architecture packet is:

- *Data Access Design Packet (APPENDIX E-1).* This design packet outlines tactical data access design principles and decisions.

The packet supports the publication architecture by highlighting specific points that meet the needs identified in the Business Requirements document.

D. DISCUSSION NOTES

The following discussion notes provide additional information and guidance for the information architecture.

- The conceptual design guidelines provide the tactical design decisions that guide exchange construction and implementation. These guidelines will be used to structure the physical implementation characteristics.
- The key to the design is the ability to easily change or move a discrete data set whenever required.

DATA ACCESS DESIGN PACKET

This subappendix sketches the concepts and design supporting the access to information and the specific technological infrastructure that supports that access. This packet provides additional design parameters for the query components; specifically, it provides the vision and principles for the access methodology to the database. The access methodology outlined below is critical to the long-term vision of the Model County environment. The data access vision is discussed below.

A. VISION

The vision for data access relies on two primary means of access: query and direct. Direct access is the most limited method that will be used within the Model County environment and is the method currently used to obtain information from a system. It allows direct access to the information within the data store. Query access will be the most common means of access for nonsystem users. These two methods of access will be implemented at a component level such that an application suite may have four direct access components (already existing) and seven query access components (within the Model County environment). The conceptual model in EXHIBIT E-1-1, which follows this page, depicts these two data access methods. In addition, the following points guide the overall vision:

- Model County access to systems will be constructed in a modular method so that repository changes and implementation of middleware will not require changes to the data access methods.
- The end result of the access efforts will be a modular and distributed logical information repository.

The data access vision is supported by the principles outlined in the next subsection.

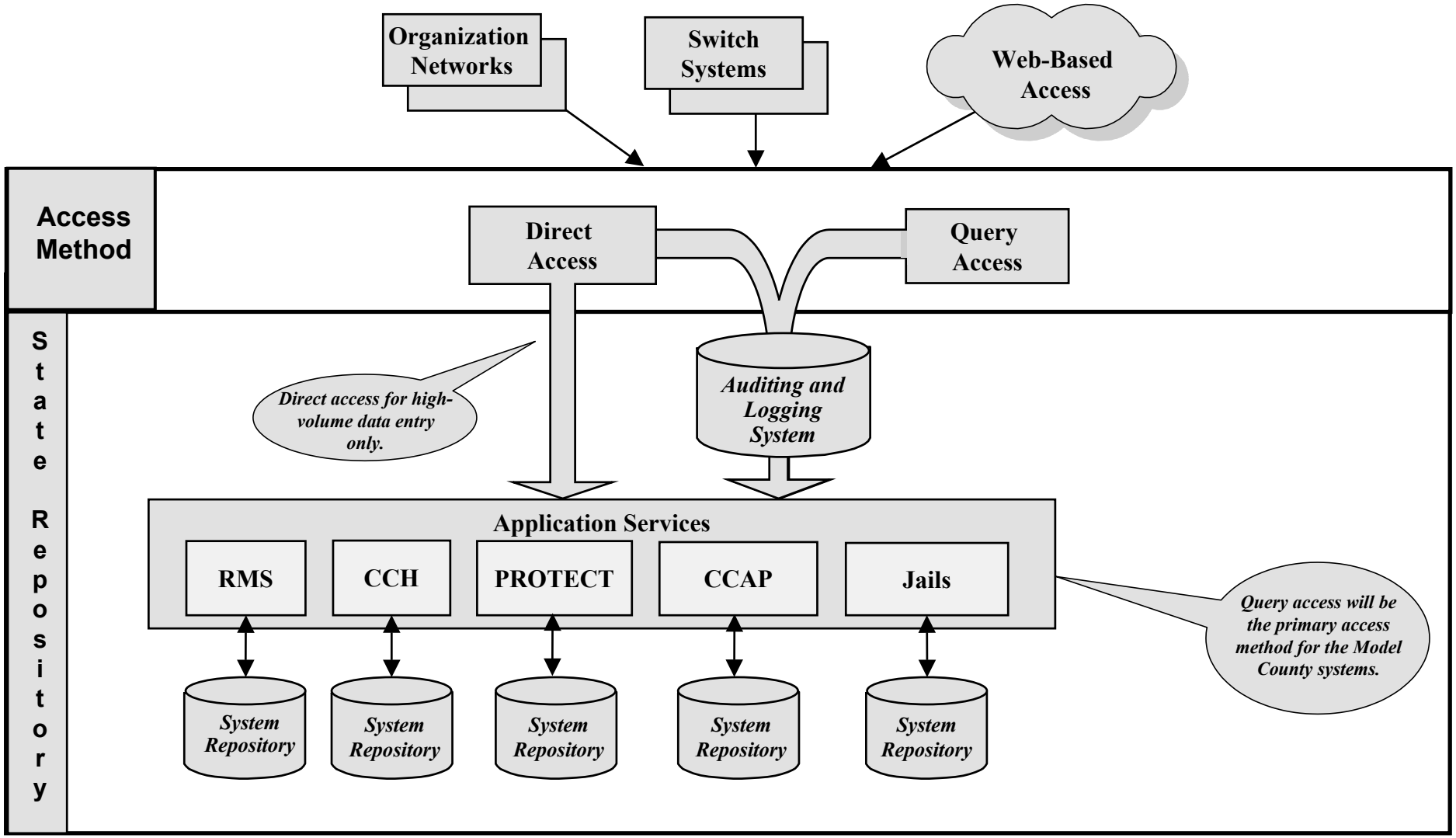
B. PRINCIPLES

The data access principles detailed below provide expanded guidelines for the vision described above and depicted in EXHIBIT E-1-1.

- Data access will occur from two primary areas: organizations and the Model County Web site. It will occur through three primary means: organization networks through the Internet,

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

DATA ACCESS



the state network connected to organization network, and Web interfaces through the Internet.

- Access should not degrade performance.
- Access will be easily maintainable.

The principles outlined above will enhance Model County project staff's abilities to implement the data access vision. The principles guide the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The conceptual design guidelines provide the tactical design decisions that guide the data access design. These guidelines will be used to structure the physical implementation characteristics of the data access methodologies. All construction and implementation choices will support the data access design outlined by the following guidelines:

- The goal of the data access design is to eventually rely directly on data from the actual system repositories.
- The central design feature of the data access methods will be through the use of specific access components.

The design decisions are supported by discussion notes described in the next subsection.

D. DISCUSSION NOTES

The discussion notes that support the data access design are outlined below.

- Application access points must be clearly documented during the design and specification phases so that the access methodology can be validated.
- Construction and implementation schema must clearly articulate the access methods that will be used for each service.
- Security within an application and the data store must support both access methods if they are utilized within that application.

These discussion notes directly affect the ease of constructing and maintaining Model County services.

APPENDIX F
INTEGRATION ARCHITECTURE PACKET

INTEGRATION ARCHITECTURE PACKET

The integration architecture is the most complex architecture of the Model County environment, yet it is the one with the fewest components. The integration architecture concepts center around a system to exchange messages, a Web site to provide the information, and a repository to store rules and some related Model County information. The architectural design to implement this straightforward concept is complex and requires an established design and clear implementation strategy. Adherence to the principles and design described in this architecture packet will minimize problems and implementation issues. EXHIBIT F-1, which follows this page,[1] provides a logical view of the integration architecture.

A. VISION

The integration architecture will support the full range of information exchange, including Push/Pull and Subscription/Notification capabilities. This architecture will be positioned to provide justice community access as well as appropriate nonjustice access for other government agencies (e.g., the Department of Health). Additional key concepts within the integration vision include:

- The portal will be deployed to allow publication of Model County information as rapidly as possible through the principles detailed in the Publication Architecture Packet (APPENDIX E).
- The message exchange is a key component for integration that will allow a system to have one interface to the message exchange, which will then determine where and how additional information exchanges will be implemented. This rule-based model will facilitate complex information transactions throughout the Model County environment.

The integration vision is supported by the principles outlined in the next subsection.

B. PRINCIPLES

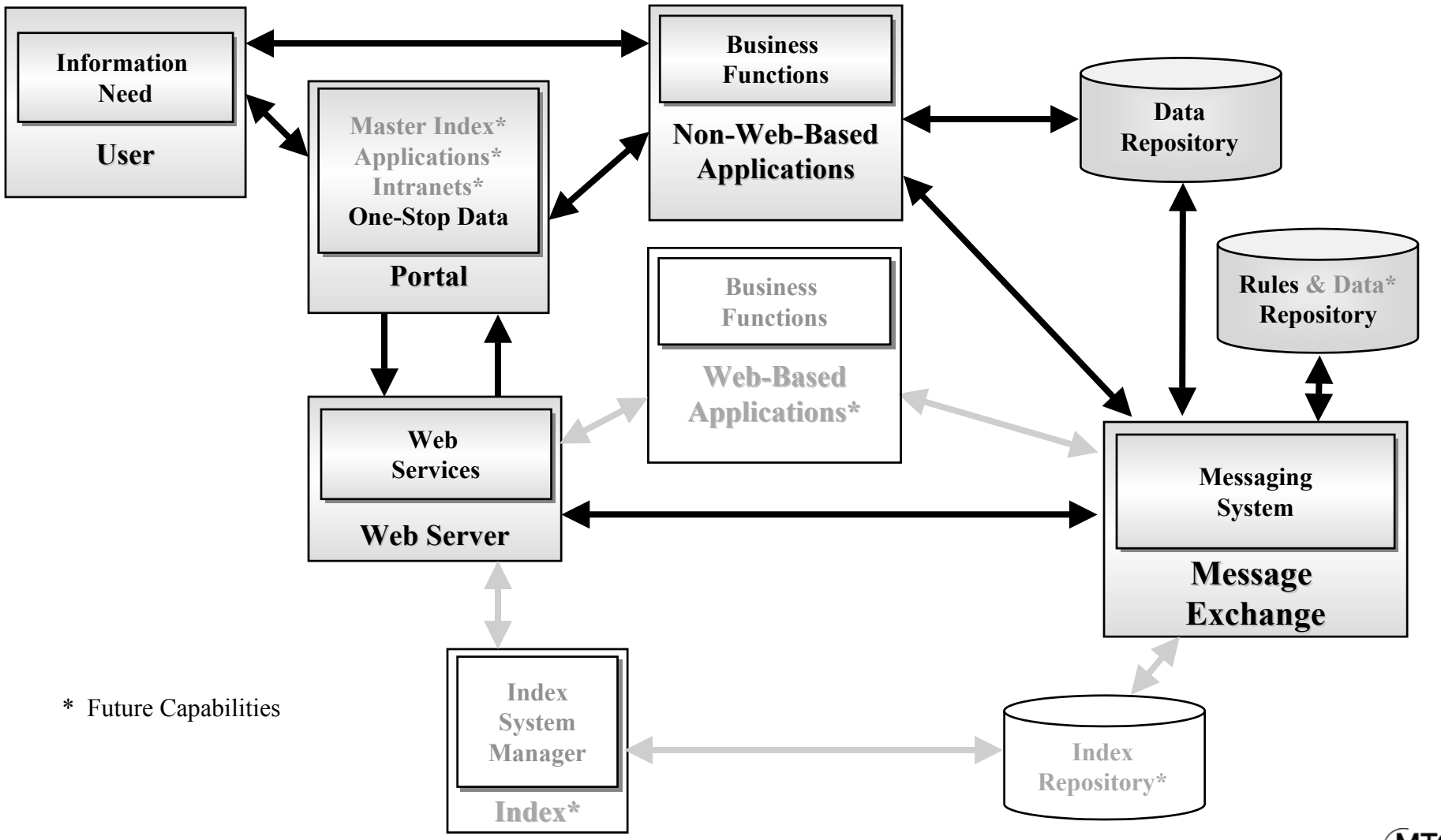
Several key design principles guide the integration architecture. These principles provide the rationale that will be used to determine design choices during the creation and implementation of integration components.

---

[1] This was also provided in Section VI of the main document as EXHIBIT VI-1.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

INTEGRATION ARCHITECTURE



* Future Capabilities

- Portal (One Stop)

  The portal will act as the Model County information broker for all user-initiated, Web-based requests for information. Although documented in APPENDIX E, the role fulfilled by the portal in the delivery of information is the central theme for the publication layer in the integration model.

- Exchange Rule Base

  An exchange rule base functions as the brain and primary logic source for the integration architecture. Rules will be defined for every piece of information that is sent to the integration backbone. The rule for a particular piece of information, called a "document" by SEARCH, will specify how the integration architecture will process the document. Several actions, called "methods" in the message exchange vernacular, are typically specified by a rule and may be an exchange, update to the index, query or response, and other actions that support partner communication. The rule base is often physically located in the Model County equipment area and Model County repository.

- Model County Repository

  The need to store the rule base and any temporary subset of data is fulfilled by the Model County repository. This is a high-availability database that only supports the Model County environment. The implementation needs of the Model County environment will dictate sizing and physical structure of the repository.

- One-to-Many Exchanges

  A key focus of the integration environment is to create one rule-based Model County-to-system interface. This interface and the Model County message exchange and supporting rule base are responsible for handling information movement from one system to another within the Model County environment. This eliminates the need to create system-to-system interfaces by replacing those needs with the ability to modify the rule base to handle the information exchanges. This greatly simplifies maintenance and support. This topology also adds a degree of quality in information moving through the integration environment since it is available for validation by other Model County organizations and utilization wherever needed.

These principles are supported by the decisions in the next subsection.

C. DESIGN DECISIONS

The following architecture decisions have been established to guide the integration efforts in support of Model County publication and information exchanges.

- Base the Message Exchange on a Transaction Server Offering

  The message exchange is a complex software application that is available on the commercial market. The Model County project will acquire a COTS transaction server to meet the requirements of the message exchange. Model County staff or contractors may then adapt the commercial software to support an integration rule base and the information exchanges identified in this Technology Architecture document. Currently, Windows 2000,[2] with its embedded transaction support, and BizTalk[3] have been selected to provide this functionality.

- Maximize XML and SOAP Protocols

  The integration topology will support XML, SOAP, and WSDL. These protocols will allow the integration to maximize the rule base by dynamically enabling rules through SOAP methodologies. In addition, the rule base should be XML-based to allow simplified maintenance and automated rule change capabilities. WSDL provides internal services descriptions without utilizing published specifications such as UDDI, a method that is exposed to external users on the Internet.

The decisions highlighted above provide overall design guidance to the information component of the application layer on the integration model included as EXHIBIT IV-2. A specific design packet for the integration architecture packets is included:

- *Message Exchange Design Packet (APPENDIX F-1).* The packet outlines message exchange design principles and decisions for the BizTalk environment. This design packet will provide partners with the information necessary to understand the interface design within the Model County information-sharing topology.

The design packet supports the integration architecture by highlighting specific points that meet the needs identified in the Business Requirements document.

---

2 *http://www.microsoft.com/windows2000/techinfo/proddoc/advserverhelp.asp*

3 *http://www.microsoft.com/biztalk/default.asp*

D. DISCUSSION NOTES

The following discussion notes provide additional information and guidance for the integration architecture:

- The design outlines a need to use Model County components within the architecture to facilitate common information contexts and simplify maintenance and administration. Although this may be achieved in the long-term Model County integration vision, the current application offerings are generally not capable of supporting this feature. Model County components should be integrated into existing applications whenever a current system feature is changed or enhanced. All acquisition efforts should require the ability to utilize the integration architecture, although most vendors will struggle initially with the concepts.
- The use of the portal may seem overly strict in terms of the environment described in the Technology Architecture document. This is not the case; rather, the intent is to utilize the Web site design presented in APPENDIX D-1 to support future links to non-Model County applications. The intent is not to physically package those applications within the environment, but simply to provide the starting point and supporting integration points.

MESSAGE EXCHANGE DESIGN PACKET

This subappendix provides draft information about the message exchange configuration. The message exchange is the central component for the information exchanges and will be fully detailed in the Technology Specifications deliverable. This subappendix is intended to provide the place holder for that information and an initial understanding of this important portion of the technology architecture.

A. VISION

The integration architecture provides the overall view of the exchange environment. The vision of the message exchange is to provide a software capability that can be graphically established and managed in support of Model County information exchanges. Additional key concepts within the message exchange include:

- Information is transferred through the secured network connections in the supporting infrastructure.
- The exchange platform allows easy connection of information and graphic connection of XML structures.
- Each transfer has identified formats that are required for successful transfers and are passed in the SOAP framework.
- Editing and validation occur at multiple levels and serve specific functions within the overall process.
- Data transfers are processed in common manner within the central exchange based on existing business logic wherever possible.

The vision is supported by the principles outlined in the next subsection.

B. PRINCIPLES

Several key design principles guide the exchange processes. These principles provide the framework for the current processes.

- Data transfer standards will follow related system needs from both the local systems and Model County infrastructures. Any difference will be processed by the message exchange.

- Auditing will occur on all exchange paths.
- Exchanges should not create excessive loads on the message exchange. Exchange size and timing will be adjusted if excessive loads occur.

The principles above guide the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The design decisions that guide information exchange construction, implementation, and maintenance are described below. These decisions will be used to structure the physical implementation characteristics of the information transfers from local agencies to the state. All construction and implementation choices will support a component data store model outlined by the related guidelines and specific transfer guidelines below:

- Information exchanges will be based on components used to share information in the rule repository.
- Existing data transfer load routines will be retrofitted to utilize the information-sharing topology and component structures as rapidly as possible as time and staff availability permits.
- Information exchanges will be separate and independent from each other, but they may operate in concert.
- Normal security standards will be maintained by all information-sharing mechanisms.
- Records management system (RMS) information will be formatted by the local system to standard formats[1] and transferred in XML.

The construction of independent information exchanges supports the overall architecture. The key to the design is the ability, whenever required, to easily change or move an information exchange without disrupting the environment. The design decisions are supported by discussion notes described in the next subsection.

[1] This will follow emerging national standards and will be documented in the Model County Technology Specifications.

D. DISCUSSION NOTES

The information exchange discussion items include the ability to sustain the transfers as they are modified or created and implemented within the CJIS environment. Additional notes are outlined below.

- Clear auditing and logging requirements must be identified for each information exchange.
- The methods used to create the data transfers will be consistent between those used with all other information exchanges.

Long-term information exchange maintainability and manageability is dependent on successful management of these issues.

APPENDIX G
ANALYSIS ARCHITECTURE PACKET

ANALYSIS ARCHITECTURE PACKET

Model County operations and management are, and will be, supported by an array of computerized information exchanges. These exchanges are key assets that may also provide information that will contribute to the analysis needs of the WIJIS partners. However, the analysis architecture is not the focus of the Model County project. There are specific features of the architecture that will assist with any subsequent design efforts to implement analysis functionality that is consistent with the architecture packet methodology used in the Model County technology architecture. The analysis architecture features that are built into the information-sharing topology are described in this appendix.

A. VISION

The analysis architecture is significant capability within the CJIS technology architecture that is not currently being deployed. It represents a mechanism to improve the decision-making processes that support the business operations of the justice enterprise. Future analysis components will be based on the infrastructure that supports Model County information exchanges, and connectors will be developed wherever possible to easily add analysis components in the future.

B. PRINCIPLES

To add analysis components effectively, the Model County project will apply the core technology principles discussed in Section IV to:

- Establish unused connections to information exchanges that can be used to feed analysis repositories.
- Document analysis opportunities as business processes are reviewed and information exchanges are created.
- Create a topology that will support analysis components within the framework that is deployed for the Model County project.

Applying the core technology principles within this framework means that the Model County project will create an information-sharing topology that exhibits the following design principles:

- Support User Business Functions

  The focus of the work done by information exchanges will support, improve, and enhance the analysis functions conducted by justice staff or will create and document the connection so that the analysis component can be implemented later.

- Minimize Maintenance Requirements

  Analysis component connections will ensure efficient use of limited technical resources by clearly providing application notes and written documentation of possible analysis connectors. This is a critical design principle given the distributed nature of the technology supported within the Model County project and current funding trends. The inclusion of comments in the developed components and strong documentation will have negligible cost impact while enhancing the future capabilities of the completed components.

- Maximize Information Sent to the Model County Information-Sharing Topology

  The information exchanges used to create or modify information within the system should contribute as much information as possible to the information-sharing topology. Although the exchange may not pass on all of the data received, it will be available to other future data structures and business processes that support the overall justice enterprise.

These principles guide the manner in which analysis components will be developed. The design decisions provided in the next subsection reflect that guidance.

C. DESIGN DECISIONS

The analysis architecture and goals outlined in Section II are supported by the core technology principles and architectural qualities for the Model County. Assumed tactical design decisions are:

- Support Evolutionary Change

  The implementation plan that supports further deployment of Model County exchanges will facilitate an evolutionary introduction of analysis tools within the technology architecture. This evolution will be based on completing existing projects, implementing publishing solutions, improving the application offerings and, finally, developing and enhancing a messaging solution. The overall objective of these changes is to increase the amount of accurate information made available to justice staff in a timely manner within the Model County community.

- Adopt Internet Architecture

  The analysis components will be based on an Internet-based architecture for all internal and external partners. Configuration decisions should be based on supporting the existing application graphical user interface, exchange business logic, and current operational data repositories wherever possible.

The decisions highlighted above provide overall design guidance to the analysis layer of the integration model described in Section IV of the main document. There are no specific design packets for the analysis architecture packet.

D. DISCUSSION NOTES

The following discussion notes should be considered in support of the information presented in the previous subsections:

- Local Application Systems

  The local systems may have local analysis capabilities that are not discussed or considered as part of this architecture packet. These systems are not the focus of the design; however, the design of any future analysis components should take into account the capabilities necessary to link to those systems to provide additional breadth to local analysis needs. In addition, similarly defined analysis methods should be used to allow comparison between local and shared information analysis.

- Web Portal

  Although discussed in Section IV and APPENDIX F, the Integration Architecture Packet, the Web portal represents a single, Web-based access point to the systems and information contained within the Model County environment. This affects the design of all analysis components in this architecture packet and any subsequent supporting design packets developed when these components are implemented.

APPENDIX H
MANAGEMENT ARCHITECTURE PACKET

MANAGEMENT ARCHITECTURE PACKET

The management architecture provides the framework for the management and support structures that will be used in the Model County technology architecture. The framework consists of the management vision and several types of tools that will help manage the Model County project efforts and implemented systems. In addition, the management architecture outlines the types of support that are envisioned for the information-sharing topology.

A. VISION

The vision for the Model County management architecture consists of three primary components that are necessary to implement the Model County:

- The project and development management tools and techniques that will create and implement Model County projects.
- The system management and quality control tools and procedures that support the operation of Model County systems.
- The security, audit, and monitoring procedures and tools that provide the validation that the Model County is secure and the information about who interacted with Model County systems or information whenever needed.

Several key IT management tools should be in place to provide the desired quality service and maintain return on the technology investment. These tools satisfy the principles below.

B. PRINCIPLES

The following principles outline the key processes and tools that are necessary to manage the Model County environment. Although the Model County may not implement tools to support these principles, clear procedures to satisfy the principle should be developed and followed by Model County project staff.

- Configuration Control

  In networks, this system gathers configuration information from all nodes on a LAN/WAN. The Model County will find the procedures and tools that support configuration control and provide stabilizing constructs to deploy and support Model County software and, more

importantly, the Model County exchange rule base. This is also critical for the security infrastructure that will be deployed.

- Enterprise Systems Management

  These procedures and software manage computer systems in an enterprise, which may include any and all of the following functions: software distribution, backup and recovery, job scheduling, virus protection, performance and capacity planning, etc. In the case of the Model County, the development platforms and software components should be managed with this type of tool.

- Asset Management

  These procedures and software collect and maintain an accurate inventory of hardware and software assets. It is often a component of the enterprise systems management software. The Model County may not have an immediate need for asset management software, but Model County assets should be managed procedurally as soon as a Model County project starts. It is expected that a straightforward Excel spreadsheet will be used to track the Model County equipment, but if more sophisticated systems are available, they should be used. This capability is not intended to audit or track partner systems.

- Project Management

  These procedures and software are used for management, scheduling, and controlling projects. Features include managing human resources; scheduling; tracking project, task, and/or resource levels; tracking issues and risks through resolution; and managing multiple projects. This type of tool set is also often used for estimating projects and determining how far along a project is.

- Storage Management

  This area includes tools and procedures that administer any or all of backup, archival, disaster recovery, and hierarchical storage management procedures within the Model County organization.

- Database Management

  These procedures and software perform the routine and automated management of databases. They should provide monitoring of critical relational database management system parameters, including status, event, and table space. Software supporting these efforts are

capable of problem detection and can take automated, corrective action when undesirable events occur.

- Internet Management

  Because Web-based applications can be very resource-intensive, encompassing many types of data, Internet management tools will help to ensure content availability. This is accomplished via site monitoring, traffic analysis, and Web server management. The critical Model County issues are the availability and performance of Model County intranet pages. These tools and procedures should focus on managing those aspects of the Model County implementation.

- Application Management

  These procedures and software manage the availability of network-centered applications within an organization, such as the Model County intranet. The purpose is to keep applications tuned and operating. In addition, the procedures and tools should assist the Model County to forecast possible failures based on historical problems and issues.

- Security Management

  These procedures and software manage the security architecture. Several systems contribute to the security systems that will be used by Model County. These systems, outlined in APPENDIX H-1, will require continual monitoring and validating efforts. An additional component of the security management principles is the mechanisms that are used to authorize, create, and manage users. The security management procedures that support the tools and systems should focus on the necessity to review access and security risks and check overall Model County security.

- Audit Management

  These procedures and software manage the auditing and logging systems. These systems also contribute to the security and tracking mechanisms used by the Model County. These systems, outlined in APPENDIX H-2, will require periodic monitoring and validating efforts. The auditing and logging management procedures that support the tools and systems should focus on the level of information that is required and actually captured by Model County auditing and logging functions.

These principles outline the significant management efforts necessary to operate the envisioned Model County systems. The following subsection highlights specific areas in which tools and procedures should be implemented.

C. DESIGN DECISIONS

The following decisions should be implemented either procedurally or with software tools available from commercial sources:

- The Model County should employ the following project and development management tools and techniques:
  - » Configuration control.
  - » Asset management.
  - » Project management.
  - » Enterprise systems management.
- The Model County should employ the following system management and quality control tools and procedures:
  - » Enterprise systems management.
  - » Storage management.
  - » Database management.
  - » Internet management.
  - » Application management.
  - » Security management.
- The Model County should employ the following security, audit, and monitoring procedures and tools:
  - » Enterprise systems management.
  - » Security management.
  - » Audit management.

These decisions will focus the management efforts into common approaches that support the Model County. The specific function designs are detailed in the following management design packets:

- *Security and User Database Design Packet (APPENDIX H-1).* This packet outlines the security and user authorization design principles and decisions.
- *Auditing and Logging System Design Packet (APPENDIX H-2).* This packet outlines the auditing and logging system design principles and decisions.

The design packets support the management architecture by highlighting specific points that meet the needs identified in the Business Requirements document.

D. DISCUSSION NOTES

The following discussion notes support the information presented in the previous subsections:

- Project management practices and policies will be an initial project in the Model County implementation road map. The project management component of the Model County plan is essential. Clear milestones and communication must exist for Model County success.
- Enterprise management tools may currently be employed by the Model County project team.
- The implementation of security and auditing procedures should be a key Model County implementation priority owing to the requirements of various Model County organizations and oversight agencies. In addition, these tools will assist Model County project teams with their efforts to initially implement security configurations.

SECURITY AND USER DATABASE DESIGN PACKET

This subappendix provides the design and conceptual structure of the user authorization and security system that manages access to information within the systems. The security system will be an important part of the Model County environment because it is the component that determines what is seen and not seen. In addition, it will provide a smooth transfer between the various system components without a need to reauthenticate between systems. The vision, principles, design decisions, and discussion notes below provide specific insight into the security and user database design.

A. VISION

The vision of the user authorization and security model is to create a single sign-on access point that controls a user's access to all components within the Model County environment. The security system may physically exist in two separate systems, as noted in EXHIBIT H-1-1, which follows this page. This exhibit depicts the user authorization and security model. The following concepts highlight the purpose of the user authorization and security design:

- The security repository will be the primary means to authenticate users and access to the systems.
- The Lightweight Directory Access Protocol (LDAP) services will be the secondary means to authenticate users and access to the systems that are currently configured for LDAP support.
- Access information will be maintained through a combination of the current LDAP service and a user interface to the security repository.

The security and user database vision is supported by the principles outlined in the next subsection.

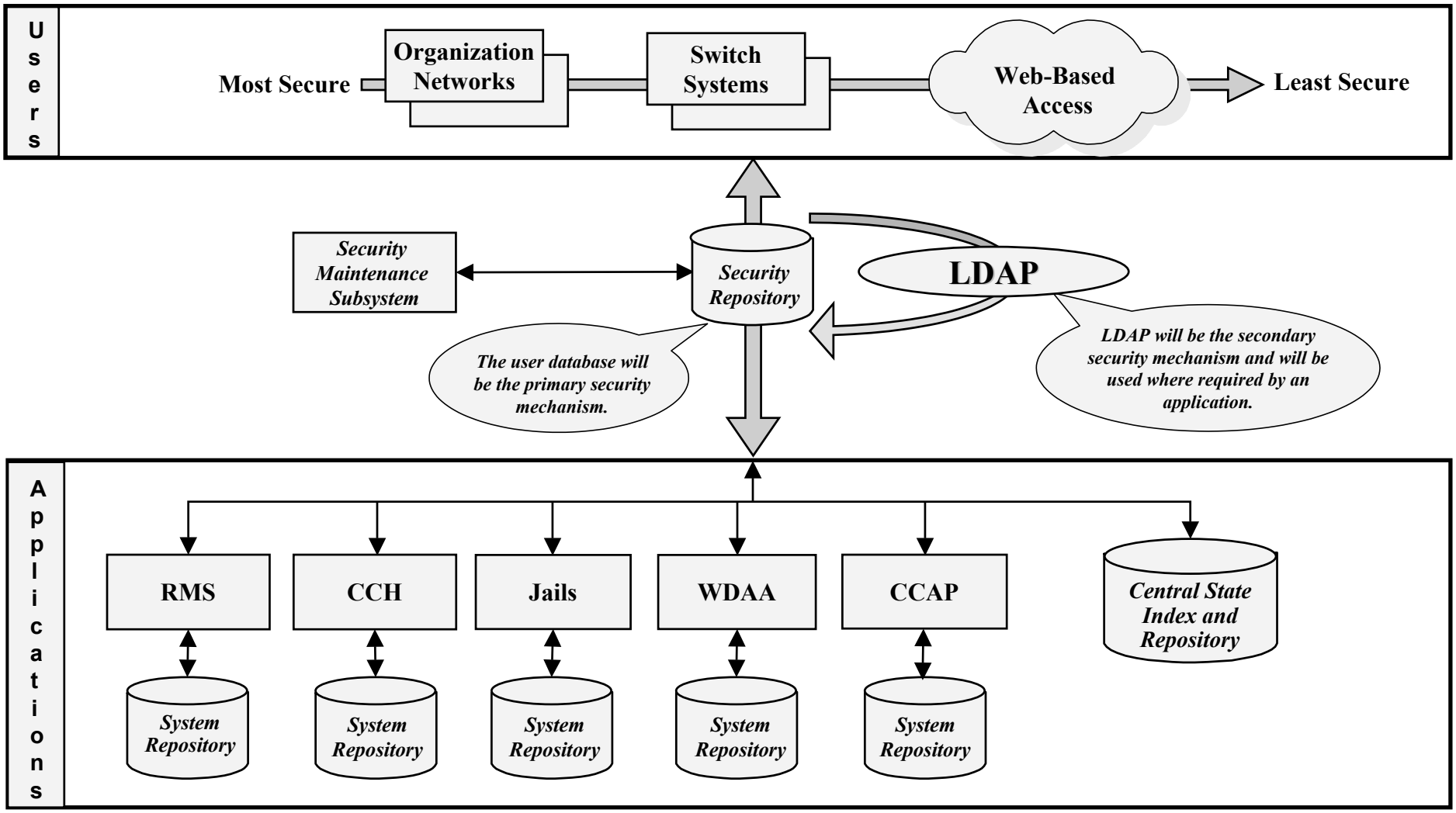
B. PRINCIPLES

As stated in the vision, the primary means to authenticate users will be based on the user security repository. The secondary means will be the existing LDAP service that is currently configured for some systems. The following principles apply to the user authorization and security model:

- When a service or system is unable to utilize the security data repository directly, it will utilize the LDAP services.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

SECURITY MODEL



MTG

- Services and systems that do not use a security data repository will be scheduled for replacement or upgrade at the earliest possible time.
- Security will primarily be maintained in the security repository for ease-of-use and maintenance.
- The security repository will be a logically separate database. This database should be moved to a physically separate database server once the Model County is extended.
- The security repository will be SQL-compliant.
- The LDAP services will be based upon Model County standards and current implementation.
- The security repository will used to populate the LDAP services information.

These principles guide the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The design decisions provide the tactical design decisions that guide the security system implementation. These design choices will be used to structure the physical implementation characteristics of the security repository and the current LDAP service-based systems. All construction and implementation choices will support the security model and are outlined by these guidelines:

- A Web-based front will be created to easily manage the information in the security repository.
- The security repository will house all non-LDAP security information, such as specific message key authorizations, application component privileges, and query permissions.
- The security repository will utilize SQL executive commands to run scripts that will apply updated security information to the LDAP service.
- Applications and query components will check the security repository for authority to execute actions against system information. This may require specific modifications to applications and services to utilize the security repository.
- Both LDAP and non-LDAP access will be annotated in the audit subsystems.

The impact is described in the discussion notes below.

D. DISCUSSION NOTES

The critical security issue that must be managed is interaction between the security repository and the LDAP services. Applications must be designed with the security repository in mind. Other discussion notes are outlined below.

- Script configuration management and maintenance must be carefully established and controlled.
- Access to the security repository must be controlled through a dedicated front end.
- Security repository access should be fully audited.

The notes require specific attention and necessitate further discussion of the auditing and logging system design, presented in APPENDIX H-2.

AUDITING AND LOGGING SYSTEM DESIGN PACKET

This subappendix provides the support structure design principles that enable full system auditing and activity logging for the Model County environment. The concept of the auditing and logging system is to create a layer that resides within all components in the Model County environment that will provide audit information about the activity within the systems. This will occur for all access methodologies and will contain defined information based on Model County business rules. The vision and concepts of the auditing and logging system are described in the following paragraphs.

A. VISION

The auditing and logging system will be a system layer between the access point and the actual information repositories. The components that comprise this layer will be focused at the point of service and component access. This creates the environment depicted in EXHIBIT H-2-1, which follows this page. The environment consists of the following key concepts:

- The Model County needs the ability to identify a user and determine that user's authorized services from a superset of authorized enterprise services.
- The actual activities accomplished by the user will be logged within the auditing system.

The auditing and logging system vision is supported by the principles outlined in the next subsection.

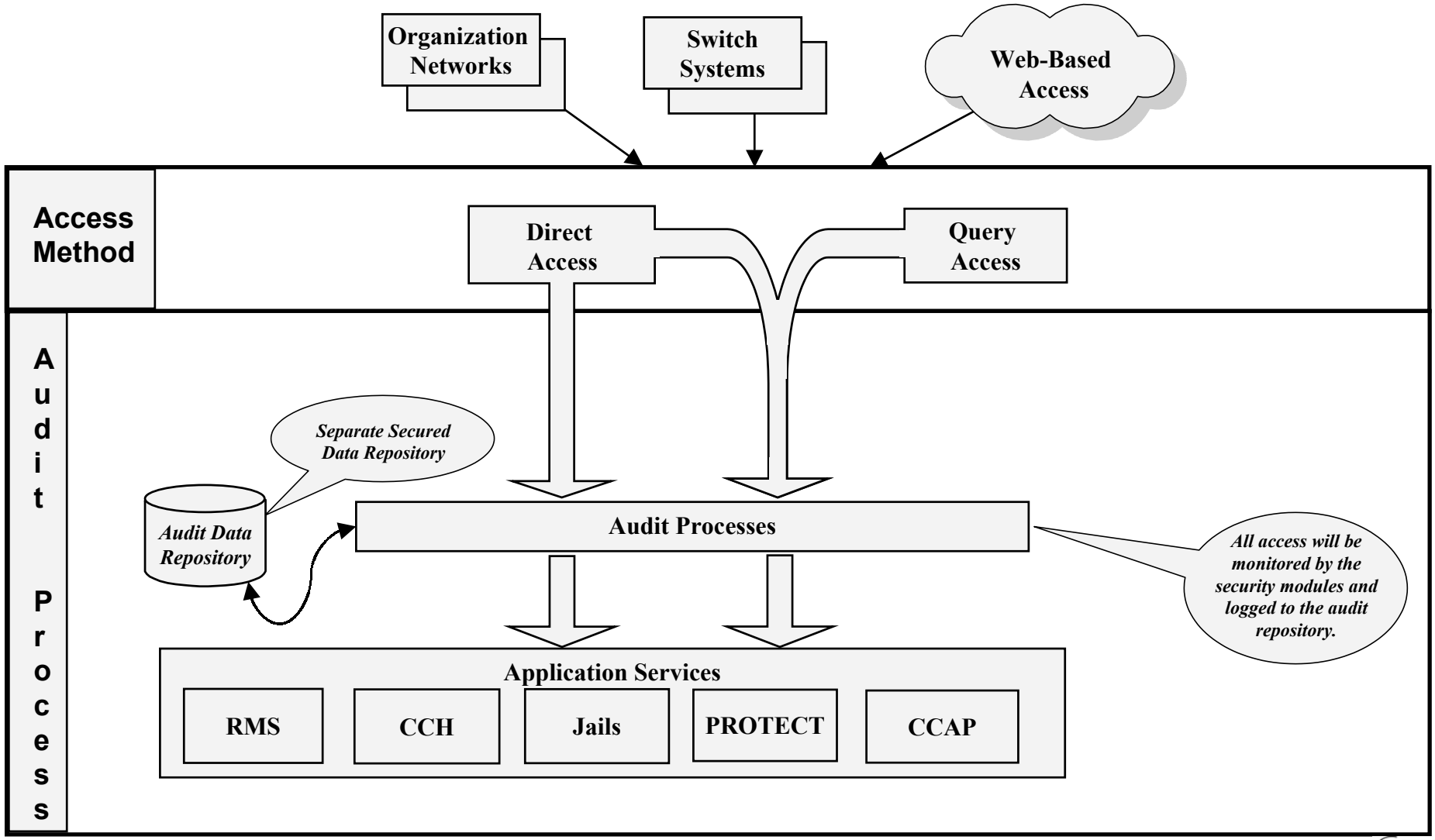
B. PRINCIPLES

The auditing and logging system will be focused on capturing user entry, activities, and exit from identified system components and services. The design of the auditing and logging system will be based on the key principle that information access will be audited unless specifically excluded from the audit routines. Other principles that provide auditing guidance and logging criteria are outlined below.

- Audit settings will be maintained from a single point of maintenance.
- A single point for security logging authority will be established for all application and enterprise system solutions.

WISCONSIN DEPARTMENT OF ELECTRONIC GOVERNMENT
MODEL COUNTY TECHNOLOGY ARCHITECTURE

AUDIT MODEL



MTG

- An easy-to-use interface will contain the maintenance routines for all auditing and logging maintenance.
- All access to the auditing and logging information will be logged in accordance will Model County policies.
- Auditing routines will not affect performance of the application services.

These principles guide the design decisions listed in the next subsection.

C. DESIGN DECISIONS

The design decisions provide the tactical design decisions that guide the auditing and logging system. These decisions will be used to structure the physical implementation characteristics of the auditing and logging system. All construction and implementation choices will support the structure outlined by these decisions.

- The auditing and logging repository will be maintained in a SQL database.
- This information will have strictly controlled access.
- An auditing process layer will exist between the access systems and the data repositories.
- Access routines will contain specific logging and auditing modules that will record audit information based on the current auditing level assigned to a function.
- Auditing routines will capture all information desired by the Model County.
- Specific auditing functions will occur at the time of access, prior to the display of any results.

The impact of these decisions is described in the discussion notes below.

D. DISCUSSION NOTES

Auditing issues must be managed within the auditing and logging system implementation effort. The specific issues that must be managed are outlined below.

- The Model County needs specific audit detailed layers that can be turned on and off by Model County system administrators.

- Audit rules must be clearly articulated within Model County policies and system documentation.
- Audit testing should occur periodically once the auditing and logging system is implemented.

The impact of the auditing and logging system will be evident in two conditions: tracking unauthorized use of information and assisting with system access and performance problems.